Avaya

User's Guide

AVAYA P332G-ML

STACKABLE SWITCH

SOFTWARE VERSION 3.9

May 2002

AVAYA

Contents

List of Figures

List of Tables

Chapter 1

Overview

The P332G-ML is a powerful Multilayer Gigabit Ethernet stackable switch. It enhances the P330 line to support high density multilayer Gigabit Ethernet solutions.

The Avaya P332G-ML has 12 GBIC (SFP) fiber-optic ports and provides Layer 2 and optional Layer 3 Gigabit Ethernet switching. The high port density and stackability make it ideal for distribution and mid-sized backbone applications where performance and reliability are more important than ever. Like other members of the Avaya P330 family, the P332G-ML is available in AC and DC versions.

The low cost and scalability of the Avaya P332G-ML allow you to deploy Gigabit Ethernet throughout your network. For the first time, all your users can benefit from the latest development in Ethernet technology.

The Avaya P332G-ML adds affordable multilayer high-density Gigabit Ethernet capabilities to the Avaya P330 stackable switching system.

Multilayer switching with QoS, Policy Management and multiple levels of security and redundancy make the Avaya P332G-ML an ideal part of a converged network.

The Avaya P332G-ML is part of the P330 line. A P330 stack can contain up to 10 switches. The stacked switches are connected using stacking sub-modules which plug into a slot in the back of the P330. They are connected using the X330SC cable or the X330LC or X330L-SC cable (if the stack is split between 2 racks). The X330RC and X330L-RC cable (if the stack is split between 2 racks) connects the top and bottom switches in the stack and provides redundancy.

The P332G-ML is ready for voice and data applications, and supports IEEE standards for VLAN Tagging, Gigabit Ethernet, Spanning Tree and Flow Control.

Avaya P332G-ML Highlights

- Up to 120 GBIC ports in a stack.
- Octaplane™ 8 Gbps stacking fabric
- Stack, Port & LAG Redundancy
- Multiple VLANs per port
- RADIUS protocol for security
- IP Multicast filtering
- Terminal and modem interface
- AC and DC versions

Layer 3

- RIP v.1, RIP v.2, OSPF. ARP, ICMP,DHCP/BOOTP relay
- VRRP and SRRP Redundancy
- Quality of Service
- Access control

Management & Monitoring

- Avaya Multi-Service Network Manager™ management
- Web-based manager
- CLI (Command Line Interface)
- RMON/SMON

Layer 2 Features

VLANs

The P332G-ML module is fully IEEE 802.1Q compliant and can handle up to 253 tagged VLANs from a range of 1 to 3071.

Multiple VLANs per Port

The P332G-ML provides the ability to set multiple VLANs per port. The three available Port Multi-VLAN binding modes are:

- **Bound to All** - the port is programmed to support the entire 3K VLANs range. Traffic from any VLAN is forwarded through a port defined as Bound to All.
- **Bound to Configured** - the port supports all the VLANs configured in the switch / stack. These may be either Port VLAN IDs (PVID) or VLANs that were manually added to the switch.
- **Statically Bound** - the port supports VLANs manually configured on it.

Link/Port Redundancy

Redundancy can be implemented between any two ports in the same stack at the link level. You can also assign redundancy between any two LAGs in the stack or between a LAG and a port. One port or LAG is defined as the primary port, and the other as the secondary port. In case the primary port link fails, the secondary port takes over.

Network Management Agent (NMA) Redundancy

Since each P332G-ML module has an integral SNMP agent, any module in a stack can serve as the stack NMA while other NMAs act as redundant agents in “hot” standby. If the “live” NMA fails then a backup is activated instantaneously.

Intermodule Redundancy

Intermodule redundancy includes all Port Redundancy functionality, and additionally maintains port integrity even when the primary port link fails as the result of a failure of the module. If the module on which the active port in an Intermodule Port Redundancy pair is located is powered down or removed from the stack, the secondary port in the Intermodule Port Redundancy pair takes over. Only one pair per stack can be set for Intermodule Port Redundancy.

Stack Redundancy

In the unlikely event that a P330 switch or Octaplane link should fail, stack integrity is maintained if the redundant cable is connected to the stack. The broken link is bypassed and data transmission continues uninterrupted. The single management IP address for the stack is also preserved for uninterrupted management and monitoring.

Spanning Tree

P332G-ML supports the IEEE 802.1D Standard Spanning Tree Protocol. This protocol detects and eliminates logical loops in the network and automatically places some ports on standby to form a network with the most efficient pathways.

Hot-Swappable

You can remove or replace any unit within the stack without disrupting operation or performing stack-level reconfiguration. You can therefore adapt the P330 to your requirements on the fly and with a down-time which is second to none.

When you remove an expansion module from the stack, all configuration definitions on expansion modules are lost.

If you wish to save configuration definitions perform the following procedure:

1 Power down the switch.
2 Remove the expansion module.
3 Insert the new module.
4 Power up the switch.

Radius Security

The Remote Authentication Dial-In User Service (RADIUS) is an IETF standard (RFC 2138) client / server security protocol. Security and login information is stored in a central location known as the RADIUS server. RADIUS clients such as the P332G-ML, communicate with the RADIUS server to authenticate users.

All transactions between the RADIUS client and server are authenticated through the use of a “shared secret” which is not sent over the network. The shared secret is an authentication password configured on both the RADIUS client and its RADIUS servers. The shared secret is stored as clear text in the client’s file on the RADIUS server, and in the non-volatile memory of the P332G-ML. In addition, user passwords are sent between the client and server are encrypted for increased security.

Port Classification

With the P332G-ML, you can classify any port as regular or valuable. Setting a port to valuable means that a link fault trap can be sent even when the port is disabled. This feature is particularly useful for the link / intermodule redundancy application, where you need to be informed about a link failure on the dormant port.

Network TIME Acquiring Protocols

The P332G-ML supports the SNTP Protocol over UDP port 123. You can choose between SNTP or TIME protocol over UDP port 37.

Link Aggregation Group (LAG)

LAG provides increased bandwidth and redundancy for critical high-bandwidth applications such as inter-stack links and connections to servers. With the P332G-ML you can aggregate the bandwidth of groups of up to four 1000Base-X ports in a LAG, or pairs of adjacent 1000Base-X ports within a group, for a maximum of 6 LAGs per switch.

IP Multicast Filtering

IP Multicast allows you to send a single copy of an IP packet to multiple destinations, and can be used for various applications including video streaming and video conferencing.

On LANs, IP Multicast packets are transmitted in MAC Multicast frames. Traditional LAN switches flood these Multicast packets to all stations in the VLAN. Multicast filtering functions may be added to the Layer 2 switches to avoid sending Multicast packets where they are not required. Layer 2 switches capable of Multicast filtering send the Multicast packets only to ports that connect members of that Multicast group. In order for this feature to operate correctly, you need in your network a router issuing IGMP queries.

Note: IP Multicast filtering will function only based on the port's VLAN ID and not based on any VLAN bound to the port.

Congestion Control

Congestion control is a key element of maintaining network efficiency as it prevents resource overload.

The P332G-ML supports congestion control on all Ethernet ports, using IEEE 802.3x Flow Control in full duplex mode.

Backup Power Supply

Each P332G-ML module comes with a Backup Power Supply (BUPS) connector. If the internal power supply fails, the P330-ML BUPS (available separately) automatically supplies power to the switch for uninterrupted operation.

Note: The BUPS used with P332G-ML units is different from the BUPS used with other P330 products

Fans

The P332G-ML module fans have integrated sensors which provide advance warnings of fan failure via management.

Software Download

P332G-ML includes a safe software download procedure in which backup code is always present.

You should perform a reset after downloading software to the Module.

Layer 3 Features

Modes of Operation

The P332G-ML has two modes of operation (in each mode, Layer 2 is always active):

- Layer 2-only mode
- Router mode and Layer 2.

Note: This section is only applicable if you either purchased a preconfigured P332G-ML or purchased a Routing License Key Certificate and activated the License Key.

Forwarding

The P332G-ML forwards IP packets between IP networks. When it receives an IP packet through one of its interfaces, it forwards the packet through one of its interfaces. P332G-ML supports multinetting, enabling it to forward packets between IP subnets on the same VLAN as well as between different VLANs. Forwarding is performed through standard means in Router mode.

Redundancy

Routing protocols naturally provide some level of redundancy. However, IP stations that are manually configured with a single 'default gateway' IP address do not naturally recover when their default gateway fails. These stations do not automatically try to use other routers or Layer-3-switches connected to the same subnet.

The P332G-ML supports two router redundancy protocols, VRRP and SRRP, to solve this problem.

Virtual Router Redundancy Protocol (VRRP)

VRRP is an IETF protocol designed to support redundancy of routers on the LAN, as well as load balancing of traffic. VRRP is transparent to host stations, making it an ideal choice when redundancy, load balancing and ease of configuration are all required.

The concept underlying VRRP is that a router can backup other routers, in addition to performing its primary routing functions. This redundancy is achieved by introducing the concept of a virtual router. A virtual router is a routing entity associated with multiple physical routers. The routing functions of the virtual router are performed by one of the physical routers with which it is associated. This router is known as the master router.

For each virtual router, VRRP selects a master router. If the selected master router fails, another router is selected as master router.

In VRRP, two or more physical routers can be associated with a virtual router, thus achieving the extreme reliability inherent in the SAFER architecture.

In a VRRP environment, host stations interact with the virtual router. They are not aware that this router is a virtual router, and they are not affected when a new router takes over the role of master router. This makes VRRP fully interoperable with every host station.

VRRP can be activated on an interface using a single command while allowing for the necessary fine-tuning of the many VRRP parameters. For a detailed description of VRRP, refer to VRRP standards and published literature.

Simple Router Redundancy Protocol (SRRP)

P332G-ML IP SRRP redundancy capabilities provide automatic backup Layer 3 switching for IP stations. P332G-ML units can be configured to back each other up so that if one fails the other will take over its forwarding functions. The backup P332G-ML is not idle. As long as both P332G-ML units are functional, traffic is shared between them. The P332G-ML modules can be in the same P330 stack or in different, connected, P330 stacks. The P332G-ML can back up another P332G-ML unit or any other router.

A P332G-ML unit configured to back up another unit monitors the other's status by polling it at configured intervals, and automatically detects when the other fails and when it becomes functional again. When detecting a failure, the backup P332G-ML sends a gratuitous ARP message that causes all stations to send their IP traffic to the backup P332G-ML MAC address instead of the failed unit MAC address. As long as it is an active backup resulting from the failure of the main unit, the backup P332G-ML answers ARP requests for the main unit, providing its own MAC address.

Policy – Quality of Service (QoS)

The P332G-ML supports QoS by using multiple priority levels and IEEE 802.1p priority tagging to ensure that data and voice receive the necessary levels of service.

The P332G-ML can enforce policy on routed packets (per packet), according to four criteria:

- The IEEE 802.1p priority tag in the incoming packet.
- The Diff-Serv byte (TOS field) in the IP header of the incoming packet.
- Matching the packet's source or destination IP address to the configured priority policy.
- Whether the packet source or destination TCP / UDP port number falls within a pre-defined range.

The P332G-ML can enforce centralized network policies using the CajunRules central policy management application.

Policy – Access Control

The P332G-ML supports Access Control policy. The P332G-ML uses policy lists containing both Access Control rules and QoS rules. The policy lists are ordered by rule indexing. Access Control rules define how the P332G-ML should handle routed packets. There are three possible ways to handle such packets:

- Forward the packet (Permit operation)
- Discard the packet (Deny operation)
- Discard the packet and notify the management station (Deny and Notify)

The P332G-ML can enforce Access Control policy on each routed packet, according to the following criteria:

- Matching the packet's source or destination IP address to the configured Access Control policy.
- Determine if the packet source or destination TCP/UDP port number falls within a pre-defined range.
- Using the ACK bit of the TCP header.

The P332G-ML access control rules are set-up using the Command Line Interface and the CajunRules central policy management application.

DHCP/BOOTP Relay

The P332G-ML supports the DHCP/BOOTP Relay Agent function. This is an application that accepts DHCP/BOOTP requests that are broadcast on one VLAN and sends them to a DHCP/BOOTP server that connects to another VLAN or a server that may be located across one or more routers that would otherwise not get the broadcast request. The relay agent handles the DHCP/BOOTP replies as well, transmitting them to the client directly or as broadcast, according to a flag in the reply message. Note that the same DHCP/BOOTP relay agent serves both the BOOTP and DHCP protocols.

When there is more than one IP interface on a VLAN, the P332G-ML chooses one of the IP addresses on this VLAN when relaying the DHCP/BOOTP request. The DHCP/BOOTP server then uses this address to decide from which subnet the address should be allocated.

When the DHCP/BOOTP server is configured to allocate addresses only from a single subnet among the different subnets defined on the VLAN, you may need to configure the P332G-ML with the relay address on that subnet so that the DHCP/BOOTP server can accept the request.

DHCP/BOOTP Relay in P332G-ML is configurable per VLAN and allows for two DHCP/BOOTP servers to be specified. In this case, it duplicates each request, and sends it to both servers. This provides redundancy and prevents the failure of a single server from blocking hosts from loading.

DHCP/BOOTP Relay in P332G-ML can be enabled or disabled.

RIP

P332G-ML supports the widely used RIP routing protocol (both RIPv1 and RIPv2). The RIPv1 protocol imposes some limitations on the network design with regard to subnetting. When operating RIPv1, you must not configure variable length subnet masks (VLMS). Each IP network must have a single mask, implying that all subnets in a given IP network are of the same size. Also, when operating RIPv1, you must not configure supernets, which are networks with a mask smaller than the natural net mask of the address class, such as 192.1.0.0 with mask 255.255.0.0 (smaller than the natural class C mask which is 255.255.255.0). For detailed descriptions of RIP refer to the standards and published literature.

RIPv2 is a new version of the RIP routing protocol, not yet widely used but with some advantages over RIPv1. RIPv2 solves some of the problems associated with RIPv1. The most important change in RIPv2 is the addition of a subnet mask field which allows RIPv2 to support variable length subnets. RIPv2 also includes an authentication mechanism similar to the one used in OSPF.

Configuration of the RIP version, 1 or 2, is per IP interface (default is version 1). Configuration should be homogenous on all routers on each subnet, i.e. there should *not* be both RIPv1 and RIPv2 routers on the same subnet. However, different IP interfaces of the P332G-ML *can* be configured with different RIP versions (as long as all routers on the subnet are configured to the same version).

RIPv2 and RIPv1 are considered the same protocol with regard to redistribution to / from OSPF and static route preferences.

OSPF

P332G-ML supports the OSPF routing protocol. P332G-ML can be configured as an OSPF Autonomous System Boundary Router (ASBR) by configuration of route redistribution. P332G-ML can be installed in the OSPF backbone area (area 0.0.0.0) or in any OSPF area that is part of a multiple areas network. However, P332G-ML cannot be configured to be an OSPF area border router itself.

The P332G-ML supports the equal-cost multipath (ECMP) feature which allows load balancing by splitting traffic between several equivalent paths.

While OSPF can be activated with default values for each interface using a single command, many of the OSPF parameters are configurable.

For a detailed description of OSPF, refer to the OSPF standards and published literature.

Static Routes

Static routes can be configured to the P332G-ML. They are never timed-out, or lost over reboot, and can only be removed by manual configuration. Deletion (by configuration) of the IP interface deletes the static routes using this interface as well.

A static route becomes inactive if the interface over which it is defined is disabled. When the interface is enabled, the static route becomes active again.

Static routes can only be configured for remote destinations, i.e. destinations that are reachable via another router as a next hop. The next hop router must belong to one of the directly attached networks for which P332G-ML has an IP interface. “Local” static routes, such as those that have no next hop, are not allowed.

Two kinds of static routes can be configured, High Preference static routes which are preferred to routes learned from any routing protocol and Low Preference static routes which are used temporarily until the route is learned from a routing protocol. By default, a static route has Low Preference.

Static routes can be advertised by routing protocols (i.e. RIP, OSPF) as described under Route redistribution.

Static routes also support load-balancing similar to OSPF. A static route can be configured with multiple next hops so that traffic is split between these next hops.

This can be used for example to load-balance traffic between several firewalls which serve as the default gateway.

Route Redistribution

Route redistribution is the interaction of multiple routing protocols. OSPF and RIP can be operated concurrently in P332G-ML. In this case, P332G-ML can be configured to redistribute routes learned from one protocol into the domain of the other routing protocol. Similarly, static routes may be redistributed to RIP and to OSPF. Route redistribution should not be configured carelessly, as it involves metric changes and might cause routing loops in the presence of other routes with incompatible schemes for route redistribution and route preferences.

The P332G-ML scheme for metric translation in route redistribution is as follows:

- Static to RIP metric configurable (default 1)
- OSPF internal metric N to RIP metric 1
- OSPF external type 1 metric N to RIP metric 1
- OSPF external type 2 metric N to RIP metric N+1
- Static to OSPF external type 2, metric configurable (default 1)
- RIP metric N to OSPF external type 2, metric N
- Direct to OSPF external type 2, metric 1.

By default, the P332G-ML does not redistribute routes between OSPF and RIP. Redistribution from one protocol to the other can be configured. Static routes are, by default, redistributed to RIP and OSPF. P332G-ML allows the user to globally disable redistribution of static routes to RIP, and separately to globally disable redistribution of static routes to OSPF. In addition, P332G-ML lets the user configure, on a per static route basis, whether the route is to be redistributed to RIP and OSPF, and what metric (in the range of 1-15). The default state is to enable the route to be redistributed at metric 1. When static routes are redistributed to OSPF, they are always redistributed as external type 2.

Route Preferences

The routing table may contain routes from different sources. Routes to a certain destination may be learned independently from RIP and from OSPF, and at the same time, a static route can also be configured to the same destination. While metrics are used to choose between routes of the same protocol, protocol preferences are used to choose between routes of different protocols.

The preferences only apply to routes for the same destination IP address and mask. They do not override the longest-match choice. For example, a high-preference static default route will not be preferred over a RIP route to the subnet of the destination.

P332G-ML protocol preferences are listed below from the most to the least preferred:

1 Local (directly attached net)
2 High-preference static (manually configured routes)
3 OSPF internal routes
4 RIP
5 OSPF external routes
6 Low-preference static (manually configured routes).

Netbios Rebroadcast

The P332G-ML can be configured to relay netbios UDP broadcast packets. This feature is used for applications such as WINS that use broadcast but may need to communicate with stations on other subnets or VLANs.

Configuration is performed on a per-interface basis. When a netbios broadcast packet arrives from an interface on which netbios rebroadcast is enabled, the packet is distributed to all other interfaces configured to rebroadcast netbios.

If the netbios packet is a net-directed broadcast (e.g., 149.49.255.255), the packet is relayed to all other interfaces on the list, and the IP destination of the packet is replaced by the appropriate interface broadcast address.

If the netbios broadcast packet is a limited broadcast (e.g., 255.255.255.255), it is relayed to all VLANs on which there are netbios-enabled interfaces. In that case, the

destination IP address remains the limited broadcast address.

Multinetting (Multiple Subnets per VLAN)

In Router Mode, most applications such as RIP and OSPF, operate per IP interface. Other applications such as VRRP and DHCP/BOOTP Relay operate per VLAN. Configuration of these applications is done in the Interface mode. When there is only a single interface (subnet) per VLAN then system behavior is intuitive since a subnet and a VLAN are the same.

If the configuration includes multiple interfaces (subnets) per VLAN things start to get complicated.

For example, if there are two interfaces over the same VLAN and you configure DHCP server on one interface it will be used also for the second interface over the same VLAN. This behavior might be less expected and in some cases wrong.

In order to prevent misconfiguration and unexpected results, the P332G-ML prevents configuration of VLAN-oriented commands on an interface unless the user explicitly requested to using the new "enable vlan commands" CLI command.

Configuration of "enable vlan commands" on an interface overrides this configuration on other interfaces that belong on the same VLAN.

This ensures that VLAN-oriented commands can be configured from one interface only.

In case there is only one interface over a VLAN, then VLAN oriented commands for this VLAN can be configured through the single interface without the need to issue the "enable vlan command" command.

Note:
1. VLAN-oriented commands that were configured affect the VLAN of the interface that was used at the time the command was issued.
2. If the interface is moved to another VLAN (using the "ip vlan command") VLAN oriented configuration still relates to the original VLAN.

Router Configuration File

The Configuration File feature allows the user to read the P332G-ML routing configuration parameters and save them to a file on the station. The routing configuration commands in the file are in CLI format. The user can edit the file (if required) and re-configure the P332G-ML by downloading the configuration file. Although the file can be edited, it is recommended to keep changes to the file to a minimum. The recommended configuration method is using Avaya Multi-Service Network Manager P330 Device Manager and/or the CLI. Changes to the configuration file should be limited to those required to customize a configuration

file from one router to suit another.

Avaya P332G-ML Standards Supported

The P332G-ML complies with the following standards.

IEEE

- 802.3x Flow Control on all ports
- 802.1q / p VLAN Tagging support on all ports
- 802.1D Spanning Tree protocol
- 803.2z Gigabit Ethernet ports

IETF - Layer 2

- MIB-II - RFC 1213
- Structure and identification of management information for TCP / IP-based Internet - RFC 1155
- Simple Network Management Protocol (SNMP) - RFC 1157
- MIB-II - RFC 1213
- PPP Internet Protocol Control Protocol (IPCP) - RFC 1332
- PPP Authentication Protocols (PAP & CHAP) - RFC 1334
- PPP - RFC 1661
- ATM Management - RFC 1695
- RMON - RFC 1757
- SMON - RFC 2613
- Bridge MIB Groups - RFC 2674 dot1dbase and dot1dStp fully implemented. Support for relevant MIB objects: dot1q (dot1qBase, dot1qVlanCurrent)
- The Interfaces Group MIB - RFC 2863
- Remote Authentication Dial In User Service (RADIUS) - RFC 2865

IETF - Layer 3

- Internet Protocol - RFC 791
- Internet Control Message Protocol - RFC 792
- Ethernet Address Resolution Protocol - RFC 826
- Standard for the transmission of IP datagrams over Ethernet - RFC 894
- Broadcasting Internet datagrams in the presence of subnets - RFC 922
- Internet Standard Subnetting Procedure - RFC 950
- Bootstrap Protocol - RCF 951
- Using ARP to implement transparent subnet gateways - RFC 1027
- Routing Information Protocol - RCF 1058
- Hosts Extensions for IP Multicasting - RFC 1112
- Requirements for Internet Hosts - Communications Layers - RFC 1122
- MIB-II - RFC 1213
- DHCP Options and BOOTP Vendor Extensions - RFC 1533

- Interoperation between DHCP and BOOTP - RFC 1534
- Dynamic Host Configuration Protocol - RFC 1541
- Clarifications and Extensions for the Bootstrap Protocol Information - RFC 1542
- OSPF Version 2 - RFC 1583
- Computation of the Internet Checksum via Incremental Update - RFC 1624
- RIP Version 2 Carrying Additional Information - RFC 1723
- RIP Version 2 MIB Extension - RFC 1724
- Requirements for IP Version 4 Routers - RFC 1812
- OSPF Version 2 Management Information Base - RFC 1850
- IP Forwarding TAble MIB - RFC 2096
- Virtual Router Redundancy Protocol - RFC 2338

Avaya P332G-ML Network Management

Comprehensive network management as a key component of today's networks. Therefore we have provided multiple ways of managing the P332G-ML to suit your needs.

P332G-ML Device Manager (Embedded Web)

The built-in P330 Device Manager (Embedded Web Manager) allows you to manage a P330 stack using a Web browser without purchasing additional software. This application works with the Microsoft® Internet Explorer and Netscape® Navigator web browsers and Sun Microsystems Java™ Plug-in.

P332G-ML Command Line Interface (CLI)

The P330 CLI provides a terminal type configuration tool for configuration of P330 features and functions. You can access the CLI locally, through the serial interface, or remotely via Telnet.

Avaya Multi-Service Network Manager™

When you need extra control and monitoring or wish to manage other Cajun Campus equipment, then the Avaya Multi-Service Network Manager network management suite is the answer. This suite provides the ease-of-use and features necessary for optimal network utilization.

- Avaya Multi-Service Network Manager is available for Windows® 95/NT®/2000 and Solaris 2.8
- Avaya Multi-Service Network Manager can operate in Stand-Alone mode with Windows® NT®/2000 and
  Solaris 2.8.
- Avaya Multi-Service Network Manager operates under HP OpenView for Windows® 95/NT®/2000.

Avaya P332G-ML Network Monitoring

RMON I MIBs - RFC 1757

- RMON I support for the following standard monitoring MIBs:
  - Statistics
  - History
  - Alarms
  - Events

SMON MIBs - RFC 2613

- SMON support for the following standard monitoring MIBs:
  - Data Source Capabilities
  - Port Copy
  - VLAN and Priority Statistics.

Bridge MIB Groups - RFC 2674

- dot1dbase and dot1dStp fully implemented.
- Support for relevant MIB objects: dot1q (dot1qBase, dot1qVlanCurrent).

DiffServ Monitoring

Monitors zero and non-zero DiffServ usage per protocol for routed packets (per DSMON IETF draft.)

Port Mirroring

The P332G-ML provides port mirroring for additional network monitoring functionality. You can filter the traffic and mirror either incoming traffic to the source port or both incoming and outgoing traffic. This allows you to monitor the network traffic you need.

Ports which are members in a Link Aggregation Group (LAG) cannot *also* be used as Port Mirroring Destination or Source ports.

SMON

The P332G-ML supports Avaya's ground-breaking SMON Switched Network Monitoring, which the IETF has now adopted as a standard (RFC2613). SMON provides unprecedented top-down monitoring of switched network traffic at the following levels:

- Enterprise Monitoring
- Device Monitoring
- VLAN Monitoring
- Port-level Monitoring

This top-down approach gives you rapid troubleshooting and performance trending to keep the network running optimally.

Note: Avaya Multi-Service Network Manager Licence is required to run SMON monitoring.

Note: You need to purchase one SMON License per P330 Stack

Avaya P332G-ML Front and Rear Panels

Avaya P332G-ML Front Panel

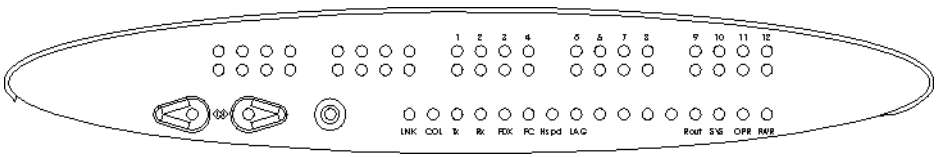
The P332G-ML front panel contains LEDs, controls, and connectors. The status LEDs and control buttons provide at-a-glance information.

The front panel LEDs consist of Port LEDs and Function LEDs. The Port LEDs display information for each port according to the illuminated function LED. The function is selected by pressing the left or right button until the desired parameter LED is illuminated. For example, if the COL LED is illuminated, then all Port LEDs show the collision status of their respective port. If you want to select the LAG function, press the right button until the LAG Function LED is lit. If you then want to select Rx, press the left button several times until the Rx function LED lights.

P332G-ML front panel shown below includes LEDs, buttons, SFP GBIC transceiver housing ports and the RJ-45 console connector (refer to Figure 2.1 and Figure 2.2). The LEDs are described in Table 2.1.

Figure 2.1 Avaya P332G-ML Front Panel

Figure 2.2 Avaya P332G-ML LEDs



Note: All LEDs are lit during a reset.

Table 2.1 Avaya P332G-ML LED Descriptions

LED Name	Description	LED Status
PWR	Power Status	OFF – Power is off
		ON – Power is on
		Blink – Using BUPS power only
OPR	CPU Operation	OFF – Module is booting
		ON – Normal operation
SYS	System Status	OFF – Module is a slave in a stack
		ON – Module is the master of the stack and the Octaplane and Redundant (optional) cable(s) are connected correctly. This LED will also light in Standalone mode.
		Blink – Box is the master of the stack and the Octaplane is in redundant mode.
ROUT	Routing Mode	OFF – Layer 2 mode
		ON – Router mode
The following Function LEDs apply to all ports		
LNK	Port Status	ON – Link is OK
COL	Collision	N / A
Tx	Transmit to line	OFF – No transmit activity
		ON – Data transmitted on line from the module
Rx	Receive from line	OFF – No receive activity
		ON – Data received from the line into the module
FDX	Full Duplex mode	Always ON

Table 2.1 Avaya P332G-ML LED Descriptions (Continued)

LED Name	Description	LED Status
FC	Flow Control	OFF – No flow control.
		ON – One of the three possible flow control modes is *enabled*.
		Note: FC LED reflects the last negotiated mode when auto-negotiation is enabled and the link is down.
Hspd	High Speed	Always ON – 1000 Mpbs mode only
LAG	Link Aggregation Group (Trunking)	OFF – No LAG defined for this port
		ON – Port belongs to a LAG

Table 2.2 Avaya P332G-ML <- -> Select buttons

Description	Function
Left / Right	Individual – select LED function (see table above)
Reset module	Press both right and left buttons together for approximately 2 seconds. All LEDs on module light up until buttons are released.
Reset stack	Press both Right and Left buttons together for 4 seconds. All LEDs on stack light up until buttons are released.

Avaya P332G-ML Back Panel

The P332G-ML back panel contains a stacking sub-module slot, power supply and BUPS connector. Figure 2.3 shows the back panel of the AC switch and Figure 2.4 shows the back panel of the DC switch with a stacking sub-module installed.

Figure 2.3 Avaya P332G-ML AC Back Panel

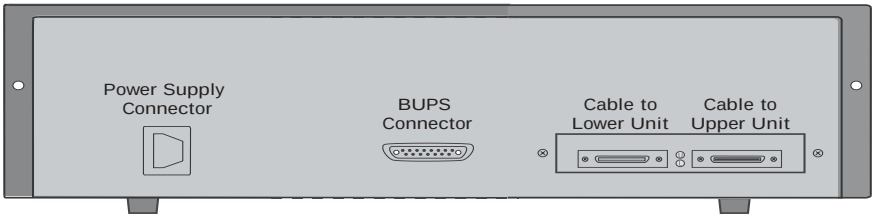
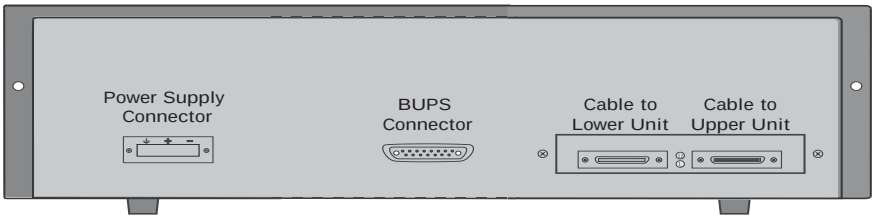


Figure 2.4 Avaya P332G-ML DC Back Panel



Note: Any further illustrations of the P332G-ML back panel will be that of the AC model shown in Figure 2.3.

BUPS Input Connector

The BUPS input connector (see Figure 2.3 and Figure 2.4) is a 3.3 V DC and 5 V DC connector for use with the P330 BUPS-ML unit only. A BUPS Input sticker appears directly above the BUPS input connector, which is covered with a metal plate.

Figure 2.5 BUPS Input Connector Sticker.

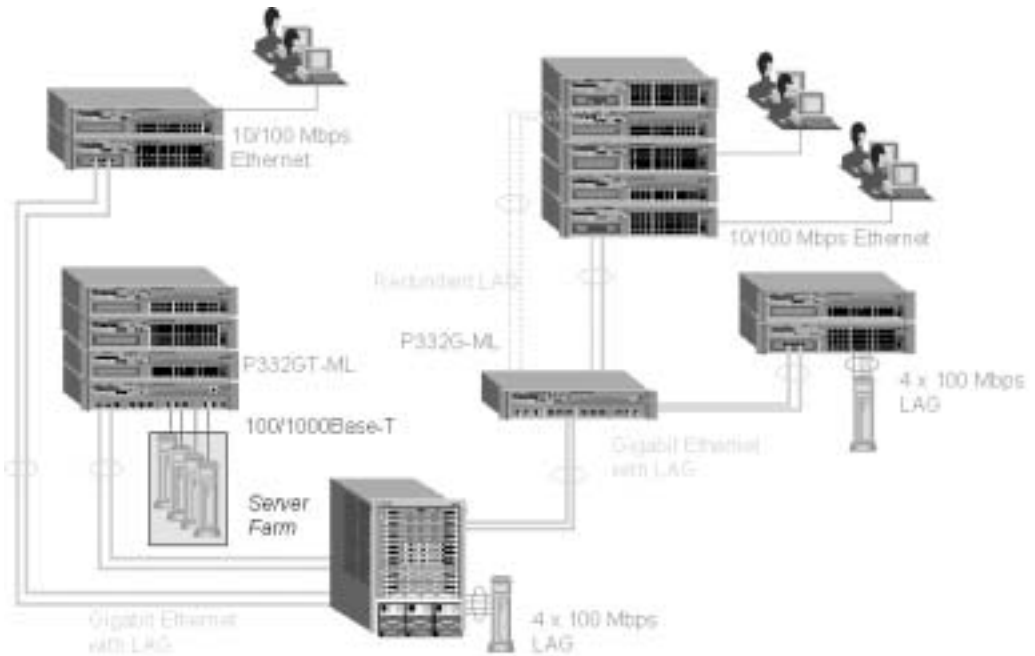
Applications

The following section describes typical applications for the P332G-ML in a network with other Cajun Campus products.

Application 1

This application shows P882 as the network backbone with P332G-ML as a distribution with LAG and redundant links.

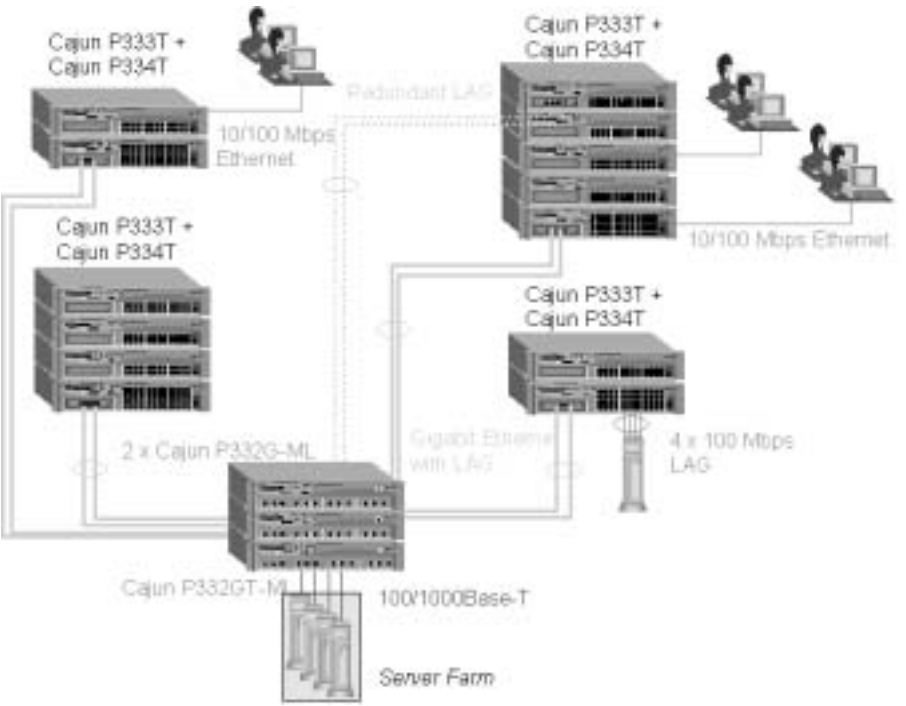
Figure 3.1 P330 stacks with a P882 backbone



Application 2

This application shows a P332G-ML as the multilayer SMB backbone, the P332GT-ML as the server farm switch and the P330 stack as closet devices

Figure 3.2 P330 stacks with a P330 backbone



Installation and Setup

The P332G-ML is ready to work after you complete the installation instructions below. The P332G-ML ports provide complete connectivity and no configuration is required to make the system work.

Installing the X330STK-ML Stacking Sub-Module

Caution: The stacking sub-modules contain components sensitive to electrostatic discharge. Do not touch the circuit board unless instructed to do so.

To install the stacking sub-module in the P332G-ML:

1 Remove the blanking plate from the back of the P332G-ML switch.
2 Insert the stacking sub-module gently into the slot, ensuring that the metal base plate is aligned with the guide rails. The metal plate of the X330STK-ML (and *not* the PCB) fits onto the guide rails.
3 Press the sub-module in firmly until it is completely inserted into the P332G-ML.
4 Gently turn the two screws on the side panel of the stacking sub-module until they are secure.

Note: The P332G-ML must not be operated with the back-slot open. The stacking sub-module should be covered with the supplied blanking plate if necessary.

Note: Only use the X330STK-ML stacking module with the P332G-ML.

Positioning

P332G-ML can be mounted alone or in a stack in a standard 19-inch equipment rack in a wiring closet or equipment room. Up to 10 units can be stacked in this way. When deciding where to position the unit, ensure that:

- It is accessible and cables can be connected easily and according to the configuration rule.
- Cabling is away from sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines and fluorescent lighting fixtures.
- Water or moisture cannot enter the unit case.
- Air-flow around the unit and through the vents in the back and sides of the case is not restricted.

Note: Use Octaplane cables to interconnect with other switches.

Rack Mounting

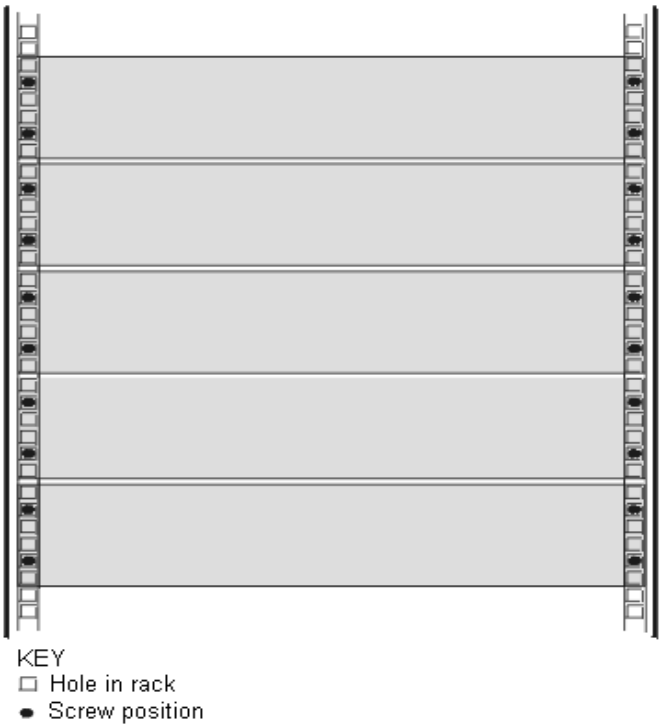
The P332G-ML case fits in most standard 19-inch racks. P332G-ML is 2U (88 mm, 3.5”) high.

Place the P332G-ML in the rack as follows:

1 Snap open the ends of the front panel to reveal the fixing holes.

2 Insert the unit into the rack. Ensure that the four P332G-ML screw holes are aligned with the rack hole positions as shown in Figure 4.1.

Figure 4.1 P332G-ML Rack Mounting



3 Secure the unit in the rack using the screws. Use two screws on each side. Do not overtighten the screws.

4 Snap close the hinged ends of the front panel.

5 Ensure that ventilation holes are not obstructed.

Connecting Stacked Switches

Note: The two ends of the Octaplane cable terminate with different connectors. Each connector can only be connected to its matching port.

The following cables are used to connect stacked switches:

- Short Octaplane cable (X330SC) – ivory-colored, used to connect adjacent switches (Catalog No. CB0223) or switches separated by a BUPS unit.
- Long / Extra Long Octaplane cable (X330LC / X330L-LC) – ivory-colored, used to connect switches from two different physical stacks, or switches separated by a BUPS unit (Catalog No. CB0225 / CB0270).
- Redundant / Long Redundant Octaplane cable (X330RC / X330L-RC) – black, used to connect the top and bottom switches of a stack (Catalog No. CB0222 / CB0269).

These are the same cables that are used with all P330 family modules.

To connect stacked switches:

Note: When adding a module to an existing stack, first connect the stacking cables and then power up the module.

1 Plug the light grey connector of the Short Octaplane cable into the port marked “to upper unit” of the bottom P330 Family module.
2 Plug dark grey connector of same Short Octaplane cable to the port marked “to lower unit” in the unit above. The connections are illustrated in Figure 4.3.
3 Repeat Steps 1 and 2 until you reach the top switch in the stack.
4 If you wish to implement stack redundancy, use the Redundant Cable to connect the port marked “ to lower unit” on the bottom switch to the port marked “to upper unit” on top switch of the stack.
5 Power up the added modules.

Caution: Do not cross connect two P330 switches with two Octaplane (light-colored) cables. If you wish to cross-connect for redundancy, use one light-colored Octaplane cable and one black redundancy cable. Figure 4.2 shows an incorrect connection.

Note: You can build a stack of up to 10 P330 switches. If you do not wish to stack all the switches in a single rack, use long Octaplane cables to connect two physical stacks as shown in Figure 4.3.

Figure 4.2 Incorrect Stack Connection

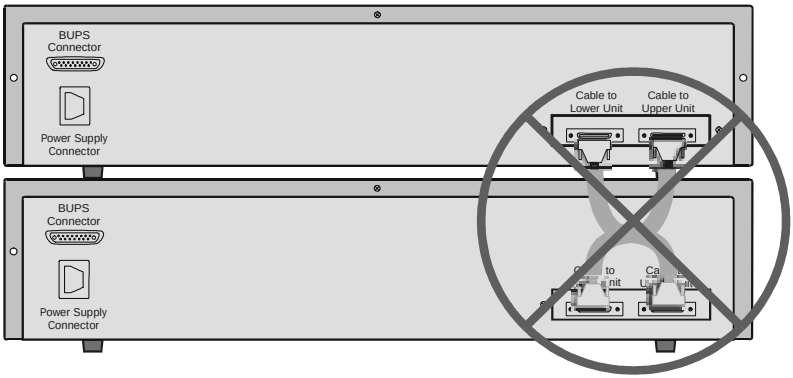
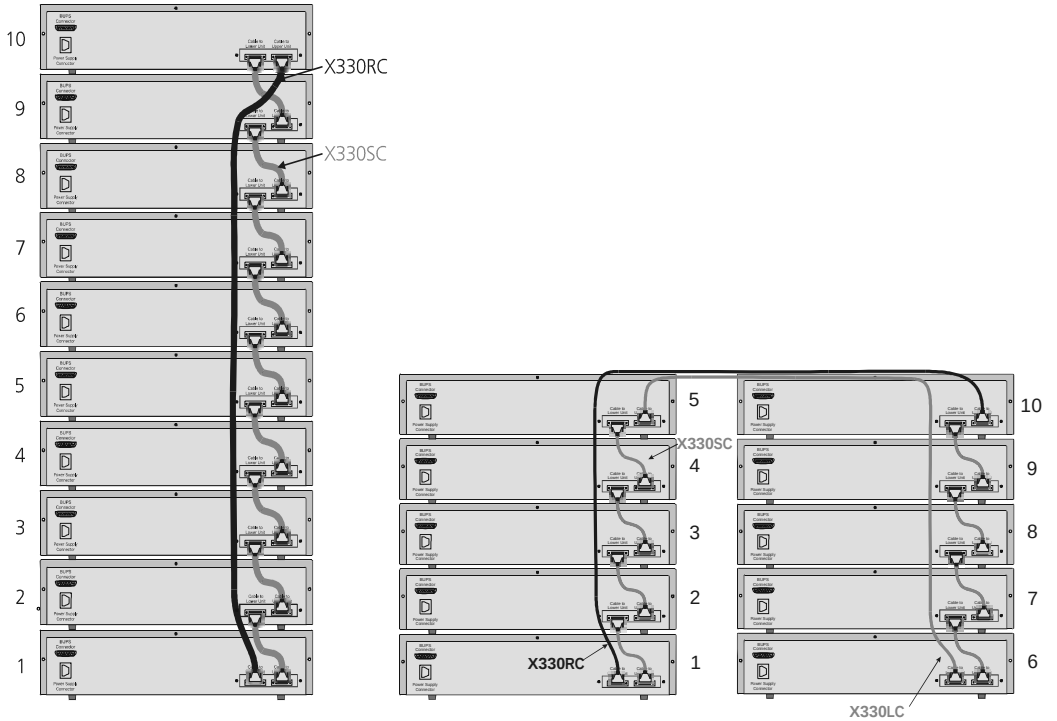


Figure 4.3 P330 Stack Connections



Powering On – P332G-ML Module AC

For the AC input version of the P332G-ML, insert the AC power cord into the power inlet in the back of the unit. The unit powers up.

If you are using a BUPS, insert a power cord from the BUPS-ML into the BUPS connector in the back of the unit. The unit powers up even if no direct AC power is applied to it.

Caution: Ensure that you connect your P332G-ML units to the BUPS-ML only. The P330 BUPS is not compatible with P332G-ML units.

After power up or reset, the P332G-ML performs a self test procedure.

Powering On – P332G-ML Module DC

For the DC input version of the P332G-ML:

1 Connect the power cable to the switch at the input terminal block. Note that:
- The terminals are marked "+", "-" and the IEC 5019a Ground symbol.
- The size of the three screws in the terminal block is M3.5.
- The pitch between each screw is 9.5mm.

Warning: Before performing any of the following procedures, ensure that DC power is OFF.

Caution: This product is intended for installation in restricted access areas and is approved for use with 18 AWG copper conductors only. The installation must comply with all applicable codes.

2 Connect the power cable to the DC power supply.

Warning: The proper wiring sequence is ground to ground, positive to positive and negative to negative. Always connect the ground wire first and disconnect it last.

After power up or reset, the P332G-ML performs a self test procedure.

Configuring the Switch

The P332G-ML may be configured using the text-based CLI, the P330 Embedded Web Manager or Avaya Multi-Service Network Manager.

For instructions on the text-based CLI, refer to Chapter 4, Cajun Campus CLI – Layer 2.

For instructions on installation of the Graphical User Interfaces (GUI), refer to Appendix A, P330 Embedded Web Manager. For instructions on the use of the graphical user interfaces, refer to the Device Manager User's Guide on the Documentation and Utilities CD.

P332G-ML Default Settings

The default settings for the P332G-ML switch and its ports are determined by the P330 software. These default settings are subject to change in newer versions of the P330 software.

Table 4.1 Default Switch Settings

Function	Default Setting
IP Address	149.49.35.214
Subnet Mask	255.255.255.0
Default gateway	0.0.0.0
Management VLAN ID	1
Spanning tree	Enabled
Bridge priority for Spanning Tree	32768
Keep alive frame transmission	Enabled
Network time acquisition	Enabled, TIME protocol
TIME server IP address	0.0.0.0
Timezone offset	0 hours
SNMP Communities Read-Only Read-Write Traps	 Public Public Public
SNMP retries number	3

Table 4.1 Default Switch Settings

Function	Default Setting
SNMP timeout	2000 Seconds
SNMP authentication trap	Disabled
CLI timeout	15 Minutes
User Name / Password	root / root

Table 4.2 Default Port Settings

Function	Default Setting
Duplex mode	Full duplex only
Port speed	1000 Mbps
Auto-negotiation[1]	Enabled
Flow control	Disabled (no pause)
Flow control advertisement	Disabled
Administrative state	Enabled
Port VLAN ID	1
Tagging mode	Clear
Port priority	0
Spanning Tree cost	4
Spanning Tree port priority	128

[1]Ensure that the other side is also set to Autonegotiation Enabled

Functions operate in their default settings unless configured otherwise.

Connecting the Cables

P332G-ML modules include the following types of ports (according to the speed and standard they support): 1000Base-SX/LX.

To connect the cables:

1 Insert an SFP GBIC (Small Form Factor Plugable Gigabit Interface Converter) transceiver (not supplied) to the port housing. For a list of approved SFP GBIC transceivers, see www.avayanetwork.com. For fiberoptic cable properties, see Table 4.3.

Note: GBICs are 3.3V.

2 Connect the Ethernet fiberoptic cable (not supplied) to the GBIC transceiver on the front panel of the Avaya P332G-ML. You can use LC or MT-RJ fiberoptic cables depending on the GBIC transceiver you are using.

3 Connect the other end of the cable to the Ethernet port of the PC, server, router, workstation, switch, or hub.

4 Check that the appropriate link (LNK) LED lights up.

Appropriate cables are available from your local supplier.

Table 4.3 displays the different types of SFP GBIC interfaces, their fiber type, diameter, modal bandwidth, wavelengths, minimum and maximum distance.

Table 4.3 Gigabit Ethernet Cabling

Gigabit Interface	Fiber Type	Diameter (µm)	Modal Bandwidth (MhzKm)	Maximum Distance (m)	Minimum Distance (m)	Wavelength (nm)
1000BASE-SX	MM	62.5	160	220	2	850
1000BASE-SX	MM	62.5	200	275	2	850
1000BASE-SX	MM	50	400	500	2	850
1000BASE-SX	MM	50	500	550	2	850
1000BASE-LX	MM	62.5	500	550	2	1310
1000BASE-LX	MM	50	400	550	2	1310
1000BASE-LX	SM	9	NA	10,000	2	1310

Connecting the Console Cable

P332G-ML has one serial port on the front panel of the switch for connecting a terminal, a terminal emulator, or a modem.

The serial port on the front panel is labelled “Console” and has a RJ-45 connector. Connect the P332G-ML to a terminal or a terminal emulator using the supplied console cable and the RJ-45 to DB-9 adaptor. To connect a modem, use the supplied cable and an RJ-45 to DB-25 adaptor.

Note: The cable and two adaptors can be found in the accessory set, and they are clearly marked.

Configuring the Terminal Serial Port Parameters

The serial port settings for using a terminal or terminal emulator are as follows:

- Baud Rate - 9600 bps
- Data Bits - 8 bits
- Parity - None
- Stop Bit - 1
- Flow Control - None
- Terminal Emulation - VT-100

Connecting a Modem to the Console Port

A PPP connection with a modem can be established only after the Avaya P332G-ML is configured with an IP address and net-mask, and the PPP parameters used in the Avaya P332G-ML are compatible with the modem’s PPP parameters.

1 Connect a terminal to the console port of the Avaya P332G-ML switch as described in Connecting the Console Cable on page 35.
2 When you are prompted for a Login Name, enter the default name **`root`**.
3 When you are prompted for a password, enter the password **`root`**. You are now in Supervisor Level.
4 At the prompt, type:
`set interface ppp <``ip_addr><net-mask>`
with an IP address and netmask to be used by the Avaya P332G-ML to connect via its PPP interface.

Note: The PPP interface configured with the `set interface ppp` command must be on a different subnet from the stack inband interface.

5 Set the baud rate, ppp authentication, and ppp time out required to match your modem. These commands are described in the “Command Line Interface” chapter.

6 At the prompt, type:
`set interface ppp enable`
The CLI responds with the following:
```
Entering the Modem mode within 60 seconds...
Please check that the proprietary modem cable is plugged
into the console port
```

7 Use the DB-25 to RJ-45 connector to plug the console cable to the modem’s DB-25 connector. Plug the other end of the cable RJ-45 connector to the Avaya P332G-ML console’s RJ-45 port.

8 The Avaya P332G-ML enters modem mode.

9 You can now dial into the switch from a remote station, and open a Telnet session to the PPP interface IP address.

Assigning P330's IP Stack Address

Note: All P332G-ML switches are shipped with the same default IP address. You must change the IP address of the master P330 switch in a stack in order to guarantee that the stack has its own unique IP address in the network.

Use the CLI to assign the P330 stack an IP address and net mask. The network management station can establish communications with the stack once this address had been assigned and the stack has been inserted into the network.

To assign a P330 IP stack address:

1 Establish a serial connection by connecting a terminal to the Master P330 switch of the stack.
2 When prompted for a Login Name, enter the default name **`root`**
3 When you are prompted for a password, enter the password **`root.`** You are now in Supervisor Level.
4 At the prompt, type:
`set interface inband` `<vlan> <ip_address> <netmask>`
Replace `<vlan>`, `<ip_address>` and `<netmask>` with the VLAN, IP address and net mask of the stack.
5 Press Enter to save the IP address and net mask.
6 At the prompt, type **`reset`** and press Enter to reset the stack. After the Reset, log in again as described above.
7 At the prompt, type **`set ip route`** `<dest> <gateway>` and replace `<dest>` and `<gateway>` with the destination and gateway IP addresses.
8 Press Enter to save the destination and gateway IP addresses.

At this point, you have assigned the P330 stack IP address and you can now configure the individual modules using either the CLI or the Avaya Multi-Service Network Manager P330 Manager.

To configure the modules using the Avaya Multi-Service Network Manager P330 Manager, see the Avaya Multi-Service Network Manager P330 Manager User Guide on the Management CD accompanying the module.

Assigning P332G-ML Initial Router Parameters

This section is only applicable if you either purchased a Layer 3 preconfigured P332G-ML module or purchased a Routing License Key Certificate for P332G-ML and activated the License Key. For information, on activating a Licence Key, see Obtaining and Activating a License Key on page 40.

To configure the initial router parameters perform the following via the CLI:

1 Enter **`set device-mode router`** and press Enter.
You will be prompted to reset the module.

2 Type **`y`**.
Wait for the module to restart and for the CLI prompt to reappear.

3 Type **`show device-mode`** and press Enter to ensure that the module is in router mode.

Note: Assign the stack IP address as described in Assigning P330's IP Stack Address on page 37 before you assign the Initial Router IP address.

4 To access Router commands from the Master module, type the command **`session`** `<module number>` **`router`** where `<module number>` is the location of the P332G-ML in the stack, and press Enter.
The command prompt changes from `Console>` to `Router-N#>` where N is the number of the router in the stack (see P330 Sessions on page 220).

5 Type **`configure`** and press Enter. The prompt `Router-N(configure)#` appears.

Note: If the IP interface is not on VLAN #1, continue with step 6, otherwise skip to step 8.

6 Create the management/routing VLAN. Use the command **`set vlan`** `<Vlan-id>` **`name`** `<Vlan-name>` replacing `<Vlan-id>` by the VLAN number, and `<Vlan-name>` by the VLAN name. Press Enter.

7 Create an IP interface name. Type:
`Router(configure)# interface <interface-name>`
Press Enter.
The **`Router(configure-if:<interface-name>)#`** prompt appears.

8 Assign the IP address and network mask of the IP interface you have created. Use the command**:**
`Router(configure-if:<interface-name>)# ip address` `<ip-address> <netmask>`
Press Enter

9 Type **`exit`** and press Enter. This returns you to the prompt:

Router(configure)#

10 If the management station is not on the same subnet as the switch, configure a default gateway (static route). Use the command: **ip default-gateway** <ip-address> and press Enter, replacing <ip-address> with the IP address of the default gateway.

11 Save the configuration changes by typing **copy running-config startup-config** and press Enter.

Obtaining and Activating a License Key

In order to benefit from Layer 3 Routing functionality, it is required that you either purchase a Layer 3 preconfigured P332G-ML module or a Routing License Key Certificate for the P332G-ML.

Each Certificate is specific for:

- The module type.
- The required feature.
- The number of devices.

After you purchase a Routing Licence Key Certificate, you must obtain and activate a Routing License Key.

Obtaining a Routing License Key

To obtain a License Key that enables routing features:

1 Go to http://license-lsg.avaya.com and click “request new license”.

2 Enter the Certificate Key and Certificate Type.

3 Click Next.

4 Enter contact information (once per certificate)

5 Click Next.

6 View number of licenses left.

7 Enter serial number of the switch(es) or module. To identify serial numbers use the CLI command:`show module-identity`.

8 Click Generate. The feature-enabling license code is generated

Activating a Routing License Key

To activate a Routing License Key:

1 Enter the acquired Routing License Key into the P332G-ML module using the `set license` CLI command.

`set license` `[module] [license] [featureName]`

where:

`module` - P332G-ML module number (the location of the switch in the stack)

`license` - license code

`featureName` - routing

and press Enter.

2 Check that the license is activated using the CLI.
Use the `show license` CLI command.

CLI – Layer 2

This chapter provides instructions for the configuration of your P332G-ML using the text-based Command Line Interface (CLI or Terminal Emulation). You can also configure your P332G-ML using the P330 Manager with its graphical user interface (see Appendix A).

The configuration procedure involves establishing a Telnet session or a serial connection and then using the P332G-ML's internal CLI. See Chapter 5 for instructions on how to establish a Telnet session or serial connection, and for a description of CLI conventions.

The CLI is command-line driven and does not have any menus. To activate a configuration option, you must type the desired command at the prompt and press Enter.

User Level Commands

This section describes all commands that are available from the User level.

Following is a table of the User Level commands and command groups (all commands are also available at the higher levels).

• `session`	Opens a session to another P330 module or X330 ATM Access module	Page 44
• `terminal width`	Display or set the width of the terminal display	Page 44
• `terminal length`	Display or set the length of the terminal display	Page 44
• `clear screen`	Clears the current terminal display	Page 45
• `show`[1]	Shows the current switch parameters	Page 46
• `ping`	Sends ICMP echo request packets to another node on the network	Page 45
• `dir`	Show files in the System	Page 74

1 This command corresponds to a group of commands and is shown in a separate
Table on Page 46

Session Command

Use the `session` command to open a session with a specific entity in a module of the stack. For example, you can open a session with the Routing entity of a P332-ML module in the stack, or with an the X330 ATM module entity plugged into a specific module.

The syntax for this command is:

`session` `[<mod_num> [switch|router|atm]]`

mod_num	(optional) The module number. If you do not specify this parameter, you will get the default entity of the stack (Layer 2 session to the Master)
switch | router | atm	(optional) The entity to which you want to open a session If you do not specify this parameter, you will get the default entity of the specific module: `switch` - Layer 2 entity of the module (see Note below) `router` - P332-ML Routing entity `atm` - X330 Access module ATM entity

Note: Layer 2 commands are only available if you open a `switch` session with the Master module.

Router commands are described in the Layer 3 CLI Chapter in this Guide.

Example:

```
P330-N# session 2 router
```

Note: When you use the `session` command the security level stays the same.

Terminal Commands

Use the `terminal width` and `terminal length` commands to set the width and length of the terminal display in characters.

The syntax for this command is:

`terminal {width|length} [<characters>]`

Clear screen Command

The clear screen command clears the current terminal display.

The syntax for this command is:

clear screen

Ping Command

Use the `ping` command to send ICMP echo request packets to another node on the network.

The syntax for this command is:

`ping [host[number]]`

host	Host IP address / Internet address of route destination. If missing then the last host IP is used.
number	Number of packets to send. If missing, then the last number is used. If the last number is not available, the default is 4.

Note: You can use this command via the Master module only.

Example:

To ping the IP number 149.49.48.1 four times:

```
P330-N> ping 149.49.48.1 4

PING 149.49.48.1: 56 data bytes
64 bytes from 149.49.48.1: icmp_seq=0. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=1. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=2. time=0. ms
P330-1(super)#  64 bytes from 149.49.48.1: icmp_seq=3. time=0. ms
----149.49.48.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Show Commands Summary Table

Following is a table of the show commands:

• show intelligent-multicast	Shows the status IP multicast filtering application	Page 72
• show intelligent-multicast hardware support	Shows whether the connected unit's hardware supports IP multicast filtering	Page 72
• show security mode	Displays the status of the MAC security feature (enabled / disabled)	Page 73
• show arp-tx-interval	Displays the keep-alive status	Page 73
• show arp-aging-interval	Displays the arp aging interval	Page 73

Show time Command

Use the `show time` command to display the current stack time.

The syntax for this command is:

`show time`

Example:

```
P330-N> show time
10:32:34 27 JAN 2000 GMT
```

Show timezone Command

Use the `show timezone` command to display the current stack timezone.

The syntax for this command is:

`show timezone`

Example:

```
P330-N> show timezone
Timezone set to 'GMT', offset from UTC is 0 hours
```

Show time parameters Command

Use the `show time parameters` command to display the status and parameters.

The syntax for this command is:

show time parameters

Example:

```
P330-N> show time parameters
Current time: L:02:49:11 02 JAN 1999 isl
Timezone set to 'isl', offset from UTC is 2 hours
Time-Server: 0.0.0.0
Time acquired from Time-Server: 0.0.0.0
Time protocol set to: TIME protocol
```

Show ip route Command

Use the `show ip route` command to display IP routing table entries.

The syntax for this command is:

show ip route

Example:

```
P330-N> show ip route

Destination    Gateway
-----------    -----------
149.49.1.1     172.20.22.201
190.20.0.0     172.20.22.202
172.20.0.0     172.20.22.96
```

Show image version Command

Use the `show image version` command to display the software version of the image on both memory banks of a specified module.

The syntax for this command is:

show image version [<mod_num>]

If no module number is specified, the image version of the all modules will be displayed.

Example:

```
P330-N> show image version 1
Mod     Module-Type                                Bank  Version
------  -----------                                ----  -------
```

```
1       24x10/100Base-T with optional expansion slot A   3.3.14
1       24x10/100Base-T with optional expansion slot B   3.5.19
```

Show download status Command

Use this command to display a summary of the last software download operation.

The syntax for this command is:

```
show download status [slot]
P330-1(super)# sh download status 1
Mod   Bank   Download State  Activity Status   Download Size
----- ------ --------------- ---------------- ---------------
1.    Bank B   idle          Download idle      0

Mod   Version   Host           File
----- --------- -------------- ------------------
1.    3.5.18    149.49.70.61 d:\p340sw\gt-ml\3.5.18\p332gt_ml
```

Show snmp Command

Use the `show snmp` command to display SNMP information.

The syntax for this command is:

`show snmp`

Example:

```
P330-N> show snmp
Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            public
read-write           public
trap                 public

Trap-Rec-Address     Traps Enabled
----------------     ----------------
1.1.1.1              config
                     fault
                    etc...
```

Show snmp retries Command

Use the `show snmp retries` command to display the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device.

The syntax for this command is:

`show snmp retries`

Example:

```
P330-N> show snmp retries
the SNMP Retries Number is 3
```

Show snmp timeout Command

Use the `show snmp timeout` command to display the default SNMP timeout in seconds. This command is useful for access using the Device Manager.

The syntax for this command is:

`show snmp timeout`

Example:

```
P330-N> show snmp timeout
the SNMP Timeout is 2000
```

Show timeout Command

Use the `show timeout` command to display the amount of time the CLI can remain idle before timing out in minutes. If the result is 0, there is no timeout limit. The default is 15 minutes.

The syntax for this command is:

`show timeout`

Example:

```
P330-N> show timeout
CLI timeout is 10 minutes
```

Show interface Command

Use the `show interface` command to display information on network interfaces.

The syntax for this command is:

show interface

Example:

To display the interface:

```
P330-N> show interface
Interface Name  VLAN    IP address          Netmask
--------------  ----  ---------------  ---------------
inband          1     10.0.0.1         255.255.255.0
ppp disable     1     0.0.0.0          0.0.0.0
```

Show device-mode Command

Use the `show device-mode` command to show the P332-ML operating mode you are currently in. Possible modes are Router, or Switch.

The syntax for this command is:

show device-mode

Show port Command

Use the `show port` command to display port status.

The syntax for this command is:

show port [<mod_num>[/<port_num>]]

mod_num	(Optional) Number of the module. If you do not specify a number, the ports on all modules are shown.
port_num	(Optional) Number of the port on the module. If you do not specify a number, all the ports on the module are shown. You can also specify a range of ports separated by a dash, e.g. 5-13 for ports 5 to 13.

Example:

To display the status for port 4 on module 3:

```
P330-N> show port 3/4
Port   Name           Status    Vlan Level  Neg     Dup. Spd. Type
------ -------------- --------- ---- ------ ------- ---- ---- -------------
 3/4   John           connected 1    4      enable  half 10M  100/1000Base-Tx
```

Show Port Output Fields

Field	Description
Port	Module and port number
Name	The name you assigned to the port
Status	Status of the port (connected, no link, disabled, no Rmt Lnk)
VLAN	VLAN ID of the port
Level	Priority level of the port (0-7)
Neg	The autonegotiation status of the port (enable, disable)
Duplex	Duplex setting for the port (fdx, hdx)
Speed	Speed setting for the port (10, 100)
Type	Port type, for example, 100BaseT, 1000BaseT, 1000BaseS

Show port trap Command

Use the `show port trap` command to display information on SNMP generic link up / down traps sent for a specific port.

The syntax for this command is:

`show port trap` [<mod_num>[/<port_num>]]

Example:

```
P330-N> show port trap 1/1
Port 1/1 up/down trap is disabled
```

Show port channel Command

Use the `show port channel` command to display Link Aggregation Group (LAG) information for a specific module or port.

The syntax for this command is:

`show port channel` [<mod_num>[/<port_num>]]

Example:

```
show port channel 1
Port   Channel Status  Channel Name
------ -------------- --------------------------------
 1/1      off
 1/2      off
 1/3      on           server1
 1/4      on           server1
------ -------------- --------------------------------
 1/5      off
 etc...
```

Show port classification Command

Use the show port classification command to display a port's classification.

The syntax for this command is:

```
show port classification [module/[port]
```

module/port	The module number/the port number

Example:

```
P330-1(super)# sh port classification

Port   Port Classification
------ ---------------------
 1/1    regular
 1/2    regular
 1/3    regular
 1/4    regular
 1/5    regular
 1/6    regular
 1/7    regular
 1/8    regular
 1/9    regular
 1/10   regular
 1/51   valuable
 1/52   valuable
```

Show port redundancy Command

Use the `show port redundancy` command to display information about all redundancy schemes defined for this stack.

The syntax for this command is:

`show port redundancy`

Example:

```
P330-N> show port redundancy
Redundancy Name     Primary Port        Secondary Port      Status
-----------------   -------------       ----------------    --------
uplink                1/7                    2/12           enable
```

Show intermodule port redundancy Command

Use the show intermodule redundancy command to display the intermodule redundancy entry defined for the stack.

The syntax for this command is:

`show intermodule port redundancy`

Example:

```
P330-N> show intermodule port redundancy
Primary-Port                : 1/1
Primary-Port status         : Disable
Secondary-Port              : 1/2
Secondary-Port status       : Disable
```

Show port mirror Command

Use the `show port mirror` command to display mirroring information for the stack.

The syntax for this command is:

`show port mirror` [<mod_num>[/<port_num>]]

Example:

```
P330-N> show port mirror
port mirroring
Mirroring both Rx and Tx packets from port 1/2 to port 1/4 is
enabled
```

Show port vlan-binding-mode Command

Use the `show port vlan-binding-mode` command to display port vlan binding mode information.

The syntax for this command is:

```
show port vlan-binding-mode [module[/port]]
```

module/port	The module number/the port number

Example:

```
P330-N> show port vlan-binding-mode
port 1/1 is statically bound
port 1/2 is statically bound
port 1/3 is statically bound
port 1/4 is statically bound
port 1/5 is statically bound
port 1/6 is statically bound
port 1/7 is statically bound
port 1/8 is statically bound
port 1/9 is statically bound
port 1/10 is statically bound
```

Show port security Command

Use the show port security command to list the security mode of the ports of a module or stack. When no port number is specified, this command displays all the secured ports in the stack.

The syntax for this command is:

`show port security` `[<module>[/<port>]]`

Example:

```
P330-N> show port security 1
Port 1/1 port security disabled.
Port 1/2 port security disabled.
Port 1/3 port security disabled.
Port 1/4 port security disabled.
Port 1/5 port security disabled.
```

```
etc.
```

Note: Port security for the P332G-ML and P332GT-ML will always have the value unknown. This command is used to display the security status for the other P330 modules in the stack.

Show internal buffering Command

This shows the size options (Maximum, Minimum, or Medium) of the Receive (Rx) buffer allocated to each port of the specified module.

The syntax for this command is:

show internal buffering [<mod_num>]

Example:

```
P330-N> show internal buffering 1
Module  Internal Buffer
------  ---------------
  1          med
```

Note: This command is not supported P332G-ML and P332GT-ML modules and should be used only for the other P330 modules in the stack .

Show boot bank Command

Use the show boot bank command to display the software bank from which the module will boot at the next boot process. This command should be issued separately for each module in the stack using the session command.

Note: This command is not supported by the P333R and P333R-LB switches.

The syntax for this command is:

show boot bank

Example:

```
Boot bank set to bank-a
```

Show module Command

Use the `show` module command to display module status and information. For each module with an expansion sub-module installed, both module and sub-module type and information are shown.

The syntax for this command is:

`show module` [<mod_num>]

mod_num	(Optional) Number of the module. If you do not specify a number, all modules are shown.

```
Mod       Type          C/S     S/N      Statuses
--- ------------------  ----  --------  ---------------------------
 1  P332GT-ML           0.0   1234567   PS:Ok Fans:Fail Mode:Layer2
    P330MLSTK           1.0             Conn-Up:Ok Conn-Down:Fail
    BUPS                                BUPS:Not Prsnt Fans:None Type:None

 2  P333T               1.0   4144162   PS:OK Fans:OK Mode:Layer2
    X330GT2             2.0
    P330STK             2.0             Conn-Up:Fail Conn-Down:Ok
    BUPS                                BUPS:Not Prsnt Fans:None Type:None
```

Output Fields

Field	Description
Mod	Module number
Type	Module Type / Expansion sub-module type
S/N	Serial number of the module
C/S	(Hardware) Configuration Symbol of the module / Expansion sub-module
Statuses	Status of the module / submodule

Show port flowcontrol Command

Use the `show port flowcontrol` command to display per-port status information related to flow control.

The syntax for this command is:

`show port flowcontrol` [<mod_num>[/<port_num>]]

Example:

```
P330-N> show port flowcontrol 3/2
Port   Send-Flowcontrol Receive-Flowcontrol
       Admin Oper       Admin Oper
------ ----- ----       ----- ----
 3/2   off   off        off   off
```

Output Fields

Field	Description
Port	Module and port number
Send-Flowcontrol-Admin	Send flow-control administration. Possible settings: • ON indicates that the local port is allowed to send flow control frames to the far end. • OFF indicates that the local port is *not* allowed to send flow control frames to the far end.
Send-Flowcontrol-Oper	Send flow-control operation mode. Possible modes: • ON indicates that the local port will send flow control frames to the far end. • OFF indicates that the local port will *not* send flow control frames to the far end.
Receive-Flowcontrol-Admin	Receive flow-control administration. Possible settings: • ON indicates that the local port will act upon flow control indications if received from the far end. • OFF indicates that the local port will discard flow control frames if received from the far end.
Receive-Flowcontrol-Oper	Receive flow-control operation mode. Possible modes: • ON indicates that the local port will act upon flow control indications received from the far end. • OFF indicates that the local port will discard flow control frames received from the far end.

Show cam Command

Use the `show cam` commands to display the CAM table entries for a specific port.

Note: MACs associated with LAGs appear under the LAG ID, not under the LAG port.

The syntax for this command is:

show cam [<mod_num>[/<port_num>]]

Example:

```
P330-N> show cam 1/1
Dest MAC/Route Dest Destination Ports
------------------ ----------------
00-40-0d-59-03-78   1/1
00-d0-79-0a-0a-da   1/1
00-40-0d-43-1e-e9   1/1
etc...
```

Show cascading fault-monitoring Command

Use the `show cascading fault-monitoring` command to display the status of the fault trap sending mode for cascading links.

The syntax for this command is:

show cascading fault-monitoring [<mod_num>]

Example:

```
P330-N> show cascading fault-monitoring 1
Module 1 cascading-down fault monitoring enabled.
Module 1 cascading-up fault monitoring enabled.
```

Show port auto-negotiation-flowcontrol-advertisement Command

The `show auto-negotiation-flowcontrol-advertisement` command displays the flowcontrol advertisement for a Gigabit port when performing autonegotiation.

The syntax for this command is:

```
show port auto-negotiation-flowcontrol-advertisement
[<mod_num>[/<port_num>]
```

[module/port] module/port number

Example:

```
P330-1(super)# show port auto-negotiation-flowcontrol-advertisement
Port 1/1  advertises no flow control capabilities.
Port 1/2  advertises no flow control capabilities.
```

Show trunk Command

Use the `show trunk` command to display VLAN tagging information of the ports, port binding mode, and the port VLAN ID.

The syntax for this command is:

`show trunk` [<mod_num>[/<port_num>]]

Example:

```
P330-N> show trunk
Port   Mode  Binding mode            Native vlan
------ ----- ---------------------- -----------
 1/1   dot1q  bound to configured vlans   1
 1/2   dot1q  bound to all vlans          1
 1/3   off    statically bound            1
 1/4   off    statically bound            1
 1/5   off    statically bound            1

P330-N> show trunk 1/5
Port   Mode  Binding mode    Native vlan Vlans allowed on trunk
------ ----- -------------- ----------- ----------------------
 1/5   off   statically bound     1       1
```

Following are the `show trunk` command output fields:

Field	Description
Port	Module and port number(s)
Mode	Tag status of the port (dot1q - dot1Q tagging mode, off - clear mode).
Binding mode	Binding mode of the port
Native VLAN	Number of the Port VLAN ID (the VLAN to which received untagged traffic will be assigned).

VLANs allowed on trunk	Range of VLAN values allowed on the port.

Show vlan Command

Use the `show vlan` command to display the VLANs configured in the stack / module.

The syntax for this command is:

```
show vlan
```

Example:

```
P330-N> show vlan
VLAN ID Vlan-name
------- --------------------------------
1       v1
5       V5
10      V10
15      V15
20      V20
25      V25
```

Show spantree Command

Use the `show spantree` command to display spanning-tree information.

The syntax for this command is:

```
show spantree [<mod_num>[/<port_num>]]
```

Example:

```
P330-N> show spantree
Spanning tree enabled
Designated Root:  00-40-0d-88-06-c8
Designated Root Priority: 32768
Designated Root Cost: 20
Designated Root Port: 1/1
Root Max Age: 20   Hello Time: 2

Bridge ID MAC ADDR: 00-40-0d-92-04-b4
```

```
Bridge ID priority: 32768




Port   State         Cost       Priority
------ ------------- ---------- ------------
1 /1   Forwarding    20         128
1 /2   not-connected 20         128
1 /3   LAG-member    20         128
1 /4   LAG-member    20         128
1 /5   not-connected 20         128
1 /6   not-connected 20         128
etc...
```

Output Fields:

Field	Description
Spanning tree	Status of whether Spanning-Tree Protocol is enabled or disabled.
Designated Root	MAC address of the designated spanning-tree root bridge
Designated Root Priority	Priority of the designated root bridge
Designated Root Cost	Total path cost to reach the root
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Bridge ID MAC ADDR	Bridge MAC address used in the sent BPDUs.
Bridge ID Priority	Bridge priority
Port	Port number

State	Spanning-tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Priority	Priority associated with the port.

Show autopartition Command

Use the show autopartition command to display the automatic partition.

The syntax for this command is:

show autopartition [module]

Example:

```
P330-N> show autopartition 1
```

Note: Autopartition for the P332G-ML and P332GT-ML will always have the value `disabled`. This command is used to display the autopartition status for the other P330 modules in the stack.

Show dev log file Command

Use the `show dev log file` command to display the encrypted device's log file.

The syntax for this command is:

show dev log file

Show log Command

Use the `show log` command to display an encrypted device's reset log.

The syntax for this command is:

show log [module]

Example:

```
P330-1(super)# sh log
MODULE 1, MESSAGE 01:
00000000 0 05002966 0205 0 0 0 0 0 0 0 0 0 0
MODULE 1, MESSAGE 02:
```

```
00000000 0 00004242 0205 0 0 0 0 0 0 0 0 0 0
MODULE 1, MESSAGE 03:
00000000 0 00002395 0205 0 0 0 0 0 0 0 0 0 0
```

Show module-identity Command

Use the show module identity command to display the module identity required for acquiring a license.

The syntax for this command is:

show module-identity [module]

Example:

```
show module-identity [module]

P330-1(super)# sh module-identity
Mod   Module Identity
---   ---------------
 1       1234567
 2       4144162
```

Show license Command

Use the show license command to display a module license.

The syntax for this command is:

show license [mod_num]

mod_num The module number

Example:

```
P330-N> show license 1
P330-N> Module 1 License:
Mod      Application            License Key             State   Feature Flag
--- ------------------ --------------------------- ---------- ------------
 1  smon               0000 0000 0000 0000 0000 0000 licensed       1
```

Show system Command

Use the show system command to display the up time, system name, location, and contact person.

The syntax for this command is:

show system

Example:

```
P330-N> show system
```

```
Uptime d,h:m:s
------------------------
0,2:40:55

System Name           System Location           System Contact
--------------------- ------------------------- -------------------------
P332_version-3.0.5   Alpha LAB                 Ygdal Naouri

Switch MAC address
------------------
00 40 0d 8a 04 b4
```

RMON Tools

Following are a series of RMON commands, however we recommend using the P330 Device Manager.

Show rmon statistics Command

This command shows the RMON statistics counters for a certain interface number according to the MIB-2 interface table numbering scheme.

The syntax for this command is:

`show rmon statistics` `<module/port>`

module / port range of ports (the default is `full switch`)

Example:

```
P330-1(super)# show rmon statistics
Statistics for switch is active, owned by Monitor
Received 171665151 octets, 1474442 packets,
1030346 broadcast and 369540 multicast packets,
0 undersize and 0 oversize packets,
1 fragments and 0 jabbers,
11 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
# of packets received of length (in octets):
64:862274, 65-127:973110, 128-255:173921,
256-511:72880, 512-1023:4374, 1024-1518:29744,
```

Show rmon history Command

This command shows the most recent RMON history log for a given History Index. The history index is defined using the `rmon history` command on Page 115 or using an RMON management tool.

The syntax for this command is:

`show rmon history` [<History Index>]

Example:

```
P330-N> show rmon history 1026
history

Entry 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 30 seconds
Requested # of time intervals, ie buckets, is 20
Granted # of time intervals, ie buckets, is 20
Sample # 1 began measuring at 2:53:9
Received 62545 octets, 642 packets,
391 broadcast and 145 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

Show rmon alarm Command

This command shows the parameters set for a specific alarm entry that was set using the rmon alarm command on Page 116 or using the P330 Device Manager.

The syntax for this command is:

`show rmon alarm` [<Alarm Index>]

Example:

```
P330-N> show rmon alarm 1026
alarm

alarm 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 60 seconds
Taking delta samples, last value was 1712
Rising threshold is 10000, assigned to event # 1054
Falling threshold is 10, assigned to event # 1054
On startup enable rising or_falling alarms
```

Show rmon event Command

This command shows the parameters of an Event entry defined by the rmon event command on Page 117 or using the P330 Device Manager.

The syntax for this command is:

show rmon event [<Event Index>]

Example:

```
P330-N> show rmon event 1054
event

Event 1054 is active, owned by amir
Description is event for monitoring amir's co
Event firing causes log and trap to community public,last fired 0:0:0
```

Show ppp session Command

Use the show ppp session command to display PPP parameters and statistics of a currently active PPP session.

The syntax for this command is:

show ppp session

Example:

```
P330-N> show ppp session
```

Show ppp authentication Command

Use the ppp authentication command to see the authentication method used for PPP sessions.

The syntax for this command is:

show ppp authentication

Example:

```
P330-N> show ppp authentication
PPP Authentication Parameters:
------------------------------
Incoming:       CHAP
```

Show ppp incoming timeout Command

Use the ppp incoming timeout command to see the amount of time in minutes that a PPP session can remain idle before being automatically disconnected.

The syntax for this command is:

show ppp incoming timeout

Example:

```
P330-N> show ppp incoming timeout
PPP incoming timeout is 10 minutes
```

Show ppp baud-rate Command

Use the show ppp baud-rate command to display the set baud-rate.

The syntax for this command is:

show ppp baud-rate

Example:

```
P330-N> show ppp baud-rate
PPP baud rate is 38400
```

Show ppp configuration

Use the show ppp configuration command to display the ppp configuration

The syntax for this command is:

show ppp configuration

Example:

```
P330-N> show ppp configuration
PPP baud rate is 38400
PPP incoming timeout is 0 minutes
PPP Authentication Parameters:
------------------------------
Incoming:       None
```

Show tftp download/upload status Command

Use the `show tftp download status` and `show tftp upload status` commands to display the status of the current TFTP configuration file copy process into / from the device.

The syntax for this command is:

`show tftp` {download|upload} **`status`** [<mod_num>]

Example:

```
P330-N> show tftp upload status 1
Module           : 1
Source file      : stack-config
Destination file : c:\conf.cfg
Host             : 149.49.36.200
Running state    : Executing
Failure display  : (null)
Last warning     : No-warning
```

Show tftp download software status Command

Use the `show tftp download software status` commands to display the status of the current TFTP Device Manager S / W (Embedded Web) download process into the device.

The syntax for this command is:

`show tftp download software status` [<mod_num>]

Example:

```
P330-1(super)# show tftp download software status
Module #1
===========
Module           : 1
Source file      : d:\p340sw\gt-ml\3.5.18\p340.web
Destination file : EW_Archive
Host             : 149.49.70.61
Running state    : Writing ...
Failure display  : (null)
Last warning     : No-warning
```

Show web aux-files-url Command

Use the `show web aux-files-url` command to display the URL / Directory from where the P330 can access the Device Management auxiliary files (for example help files).

The syntax for this command is:

`show web aux-files-url`

Show intelligent-multicast command

Use the show intelligent-multicast Command to display the intelligent multicast configuration.

The syntax for this command is:

`show intelligent-multicast`

Example:

```
P330-N> show intelligent-multicast
Intelligent-multicast configuration:
------------------------------------
intelligent-multicast state ---------------------- Disabled
Intelligent-multicast client-port-pruning time --- 600[Sec]
Intelligent-multicast router-port-pruning time ---1800[Sec]
intelligent-multicast group-filtering-delay time -  10[Sec]
Intelligent-multicast HW configuration:
#  Module           Sub-Module            Cascade
   -------          ----------            --------
1 No IPMc Support   Not Installed        No IPMc Support
```

Show intelligent-multicast hardware-support Command

Use the `show intelligent-multicast hardware-support` command to display the intelligent multicast hardware support configuration.

The syntax for this command is:

`show intelligent-multicast hardware-support`

Example:

```
P330-N> show intelligent-multicast hardware support
Intelligent-multicast HW configuration:
```

```
#  Module          Sub-Module             Cascade
   -------         ----------             --------
1 Support IPMc   Not Installed          Support IPMc
```

Show security mode Command

Use the `show security mode` command to display the status of the MAC security feature.

The syntax for this command is:

`show security mode`

Example:

```
P330-N> show security mode
Security mode enabled.
```

Note: Layer 2 commands are only available if you open a `switch` session with the Master module.

Note: The Show security mode command does not apply to the P332G-ML and P332GT-ML, and relates only to the other P330 modules in the stack.

Show arp-tx-interval Command

Use the show arp-tx-interval command to display the keep-alive frames transmission interval.

The syntax for this command is:

`show arp-tx-interval`

Example:

```
P330-N> show arp-tx-interval
ARP tx interval is set to 5 seconds.
```

Show arp-aging-interval Command

Use this command to display the arp aging interval.

The syntax for this command is:

`show arp-aging-interval`

Example:

```
P330-N> show arp-aging-interval
ARP aging interval was set to 10 minutes.
```

Dir Command

The `dir` command is used to show the file types that have been downloaded to the module.

The syntax for this command is:

`dir` [<mod_num>]

Example:

```
P330-N> dir
M# file            ver num  file type     file location  file description
-- ----           --------  ----------    -------------  ----------------
1  Booter_Image    3.5.17    SW BootImage  Nv-Ram         Booter Image
1  module-config   N/A       Running Conf  Ram            Module Configuration
1  stack-config    N/A       Running Conf  Ram            Stack Configuration
1  EW_Archive      N/A       SW Web Image  Nv-Ram         Web Download
2  Booter_Image    3.2.5     SW BootImage  Nv-Ram         Booter Image
2  module-config   N/A       Running Conf  Ram            Module Configuration
2  EW_Archive      N/A       SW Web Image  Nv-Ram         Web Download
```

Output Fields:

Field	Description
M#	The module number
file	There are several files loaded into modules memory: • module-config – file which contains the configuration settings made to this module. • stack-config – file which contains the configuration settings made at the stack level (for example IP address of the stack) • EW_Archive – file which contains the Device Manager (Embedded Web) software.
ver num	S/W Version number – relevant only for the Device Management S/W

file type	There are several file types: • Running Conf – the configuration currently in use. This is also the startup configuration in the P332-ML. • SW Web Image – Device Manager S/W archive file
file location	Type of internal memory into which the file is loaded
file description	Description of the file

Note: If the N/A is displayed for the EW_Archive file this means that the Device Manager S/W is not loaded correctly. Download the Device Manager S/W again.

Privileged Level Commands

Following is a table of the Privileged Level commands. This level includes all the commands from the User Level described above (see the User Level Commands Section for a description of these common commands).

• no hostname	Return the prompt to its default	Page 77
• no rmon history	Deletes an existing history entry	Page 77
• no rmon alarm	Deletes an existing alarm entry	Page 77
• no rmon event	Deletes an existing event entry	Page 77
• hostname	Displays or sets a new prompt	Page 78
• clear[1]	Clears current settings (group of commands)	Page 78
• set[2]	Set the module parameters (group of commands)	Page 82
• sync time	Synchronizes the time between modules	Page 111
• get time	Gets the time from the time server	Page 114
• reset	Restarts the system or a module	Page 114
• nvram initialize	Initialize the NVRAM to its factory defaults	Page 115
• configure	Currently not used in the Layer 2 CLI.	Page 115
• rmon history	Creates a history entry	Page 115
• rmon alarm	Creates an alarm entry	Page 116
• rmon event	Creates an event entry	Page 117
• copy stack-config tftp	Upload stack configuration to a file (using tftp). The file must exist before you Upload.	Page 117
• copy module-config tftp	Upload module configuration to a file (using tftp). The file must exist before you Upload.	Page 118
• copy tftp stack-config	Download a stack configuration file (using TFTP) into the device	Page 119
• copy tftp module-config	Download a module configuration file (using TFTP)	Page 120

• copy tftp EW_Archive	Download the Device Manager S/W (Embedded Web Archive file), using TFTP, into the device	Page 120
• copy tftp SW_image	Updates the software image and device manager application of a designated module	Page 121
• radius authentication[3]	Sets radius authentication parameters	Page 122

1 The `clear` command corresponds to a group of commands and is shown in a separate Table on Page 78.
2 The `set` command corresponds to a group of commands and is shown in a separate Table on Page 82.
3 The `radius authentication` commands corresponds to a group of commands listed on Page 122.

No hostname Command

Use the `no hostname` command to return the CLI prompt to its default.

The syntax for this command is:

`no hostname`

No rmon history Command

Use the `no rmon history` command to delete an existing RMON history entry.

The syntax for this command is:

`no rmon history <History Index>`

No rmon alarm Command

Use the `no rmon alarm` command to delete an existing RMON alarm entry.

The syntax for this command is:

`no rmon alarm <Alarm Index>`

No rmon event Command

Use the `no rmon event` command to delete an existing RMON event entry.

The syntax for this command is:

`no rmon event <Event Index>`

Hostname Command

Use the `hostname` command to change the Command Line Interface (CLI) prompt. The current module number always appears at the end of the prompt.

The syntax for this command is:

`hostname` `[<hostname_string>]`

hostname_string	**none** – displays current hostname **string** – the string to be used as the hostname (up to 20 characters).

Clear Commands Summary Table

Following is a Table of the Privileged Level `clear` commands.

Clear timezone Command

Returns the timezone to its default, Coordinated Universal Time (UTC)

Clear ip route Command

Use the `clear ip route` command to delete IP routing table entries.

The syntax for this command is:

`clear ip route` `<destination> <gateway>`

destination	IP address of the network, or specific host to be added
gateway	IP address of the router.

Example:

To delete the route table entries using the clear ip route command:

```
P330-N# clear ip route 134.12.3.0 192.1.1.1
Route deleted.
```

Clear snmp trap Command

Use the `clear snmp trap` command to clear an entry from the SNMP trap receiver table.

The syntax for this command is:

`clear snmp trap` `{<rcvr_addr>|all}`

rcvr_addr	IP address or IP alias of the trap receiver (the SNMP management station) to clear.
all	Keyword that specifies every entry in the SNMP trap receiver table

Example:

```
P330-N# clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
```

Clear vlan Command

Use the `clear vlan` command to delete an existing VLAN and return ports from this VLAN to the default VLAN #1. When you clear a VLAN, all ports assigned to that VLAN are assigned to the default VLAN #1.

The syntax for this command is:

`clear vlan` `<vlan-id>[`**`name`** `<vlan_name>]`

vlan_id	Number of the VLAN (range is 1to 3071).
vlan_name	VLAN name

Example:

This example shows how you can delete an existing VLAN (VLAN 5) from a management domain:

```
P330-N# clear vlan 5 name V5
This command will assign all ports on vlan 5 to their default
in the entire management domain
 - do you want to continue (Y/N)?  y
All ports on vlan-id 5 assigned to default vlan.
VLAN 5 was deleted successfully.
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Clear dynamic vlans Command

Use the `clear dynamic vlans` command to clear dynamic vlans. Only the VLANs learned by the module from incoming traffic are cleared using this command.

The syntax for this command is:

`clear dynamic vlans`

Example:

```
P330-N# clear dynamic vlans
This command will delete all the vlans that were dynamically
learned by the device - do you want to continue (Y/N)?
```

Clear port static-vlan Command

Use the `clear port static-vlan` command to delete VLANs statically configured on a port.

The syntax for this command is:

```
clear port static-vlan [module/port range][vlan num]
```

module / port range	Port range
vlan num	The VLAN to unbind from the port

Example:

```
P330-1(super)# clear port static-vlan 1/10 5
VLAN 5 is unbound from port 1/10
```

Clear cam Command

Use the `clear cam` command to delete all entries from the CAM table.

The syntax for this command is:

```
clear cam
```

Example:

```
P330-N# clear cam
CAM table entry cleared.
```

Clear log Command

Use the `clear log` command to delete the Log file of a module.

The syntax for this command is:

```
clear log [<mod_num>]
```

Clear port mirror Command

Use the `clear port mirror` command to cancel port mirroring.

The syntax for this command is:

```
clear port mirror <source-module>/<source-port>/<dest-module>/<dest-port>
```

Example:

```
P330-N# clear port mirror 1/2/1/4
this command will delete the port mirror entry
 - do you want to continue (Y/N)?  y
Mirroring packets from port 1/2 to port 1/4 is cleared
```

Set Commands Summary Table

Following is a Table of the Privileged Level `set` commands.

• set intelligent-multicast router-port-pruning time	Sets the aging time for router ports	Page 111
• set intelligent-multicast group-filtering-delay time	Sets the time delay before a filter is applied to a specific group	Page 112
• set security mode	Enables or disables the stack's MAC security	Page 112
• set arp-aging-interval	Sets the arp aging interval	Page 112
• set arp-tx-interval	Sets the keep-alive interval	Page 113
• set welcome message	Sets a welcome message to appear after a reboot.	Page 113

Set logout Command

The `set logout` command is used to set the number of minutes until the system automatically disconnects an idle session.

The syntax for this command is:

`set logout` `<timeout>`

timeout	Number of minutes (0 to 999) until the system automatically disconnects an idle session. Setting the value to 0 disables the automatic disconnection of idle sessions (default is 15 minutes).

Example:

To set the number of minutes until the system disconnects an idle session automatically:

```
P330-N# set logout 20
Sessions will be automatically logged out after 20 minutes of
idle time.
```

To disable the automatic disconnection of idle sessions:

```
P330-N# set logout 0
Sessions will not be automatically logged out.
```

Set timezone Command

Use the `set timezone` command to assign a timezone name and set the time difference of your P330 relative to the Coordinated Universal Time (UTC / GMT).

The minutes parameter can only be set to 30.

The syntax for this command is:

```
set timezone <zone_name> <hours | hours:min>[:30]
```

Example:

```
set timezone GMT -3:30
Timezone set to 'GMT', offset from UTC is -3:30 hours
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set time protocol Command

Use the set time protocol command to set the protocol for use in the system as either SNTP protocol or TIME protocol.

The syntax for this command is:

```
set time protocol  [sntp-protocol|time-protocol]
```

Example:

```
P330-N# set time protocol sntp-protocol
The protocol has been set to SNTP protocol

P330-N#  set time protocol time-protocol
The protocol has been set to TIME protocol
```

Set time server Command

The `set time server` command is used to set the TIME server address.

The syntax for this command is:

```
set time server <ip>
```

ip	IP address of the TIME server.

Set time client Command

The `set time client` command is used to enable or disable the periodic network time acquisition by the switch from the network time server (SNTP or

TIME protocol).

The syntax for this command is:

set time client <enable|disable>

Set ip route Command

Use the `set ip route` command to add IP addresses to the IP routing table. You can configure from one to ten (10) default gateways for a P330 stack.

The syntax for this command is:

set ip route <destination> <gateway>

destination	IP address of the network, or specific host to be added
gateway	IP address of the router.

Example:

This example shows how to add a default route to the IP routing table:

```
P330-N# set ip route 0.0.0.0 192.168.1.1
destination = 0.0.0.0  gateway = 192.168.1.1

ROUTE NET TABLE
destination      gateway          flags  Refcnt  Use           Interface
------------------------------------------------------------------------
0.0.0.0          192.168.1.1      1      1       3199          se0
127.1.1.0        127.1.1.1        1      8       7606          se1
------------------------------------------------------------------------

ROUTE HOST TABLE
destination      gateway          flags  Refcnt  Use           Interface
------------------------------------------------------------------------
127.0.0.1        127.0.0.1        5      2       131           lo0
10.10.10.10      192.168.1.1      7      0       0             se0
------------------------------------------------------------------------
```

Set snmp community Command

Use the `set snmp community` command to set or modify the module's snmp community strings.

The syntax for this command is:

```
set snmp community <access_type> [community string]
```

access type	read-only, read-write, or trap

Example:

```
P330-1(super)# set snmp community read-only read
SNMP read-only community string set
```

Set snmp trap Commands

Use the `set snmp trap` commands to add an entry into the SNMP trap receiver table and to enable or disable the different SNMP traps for a specific receiver. First add the `rcvr_addr` and then enable / disable the different traps for it.

The syntax for this command is:

```
set snmp trap <rcvr_addr>
set snmp trap <rcvr_addr> {enable|disable} {all|config|fault|...}
```

enable	Activate SNMP traps
disable	Deactivate SNMP traps
all	(Optional) Specify all trap types
config	(Optional) Specify the ConfigChange trap from the TRAP-MIB.
fault	(Optional) Specify the Fault trap from the TRAP-MIB.
rcvr_addr	IP address or IP alias of the system to receive SNMP traps

Example:

To enable SNMP ConfigChange traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 enable config
SNMP config change traps enabled.
```

To enable all traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 enable all
All SNMP traps enabled.
```

To disable SNMP config traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 disable config
SNMP config traps disabled.
```

To add an entry in the SNMP trap receiver table with default:

```
P330-N# set snmp trap 192.168.173.42
SNMP trap receiver added.
```

Set snmp trap auth Command

Use the `set snmp trap auth` commands to enable / disable the sending of SNMP traps upon SNMP authentication failure.

The syntax for this command is:

`set snmp trap` {enable|disable} **`auth`**

Example:

```
P330-N# set snmp trap enable auth
Authentication trap enabled
```

Set snmp retries Command

Use the `set snmp retries` command to set the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device.

The syntax for this command is:

`set snmp retries` <number>

Set snmp timeout Command

Use the `set snmp timeout` command to set the SNMP timeout in seconds. This command is useful for access using the Device Manager.

The syntax for this command is:

`set snmp timeout` <number>

Set system location Command

Use the `set system location` command to set the mib2 system location MIB variable.

The syntax for this command is:

`set system location` [<string>]

string	Location name. The location name is cleared if this field is left blank. A string of 2 words or more must be type in quotation marks – e.g. “Operations Floor”.

Set system name Command

Use the `set system name` command to set mib2 system name MIB variable.

The syntax for this command is:

`set system name` [<string>]

string	System name. The system name is cleared if this field is left blank. A string of 2 words or more must be type in quotation marks – e.g. “Backbone Stack”.

Set system contact Command

Use the `set system contact` command to set mib2 system contact MIB variable.

The syntax for this command is:

`set system contact` [<string>]

string	Contact person. The contact person field is cleared if this field is blank. A string of 2 words or more must be type in quotation marks – e.g. “Yigdal Naouri”.

Set device-mode Command

Use the `device-mode` command to change the Basic Mode of Operation of the P332-ML Module between Router and Layer 2 modes.

The syntax for this command is:

`set device-mode` `<mode>`

mode	Router | Layer2

Set interface Command

Use the `set interface` command to configure the management interface on the Master agent of the stack.

The syntax for this command is:

`set interface inband` `<vlan> <ip_addr> <netmask>`

inband	Interface name used for the management
vlan	The number of the VLAN to be used for management
ip_addr	IP address used for managing the stack
netmask	Subnet mask of the management interface

Example:

```
P330-N# set interface inband 1 192.168.42.252 255.255.255.0
Interface inband IP address set.
You must reset the device in order for the change to take effect.
```

Set interface ppp Command

Use the set interface ppp command to configure the P330 PPP interface IP parameters, exit modem mode, disconnect the PPP session, or reset the connected modem.

A PPP connection can be established only after the P330 is configured with an IP address and net-mask. The IP address is a dummy address that is shared between two peers, and must be taken from a subnet that is different from the agent's IP subnet.

The syntax for this command is:

set interface ppp <ip_addr><net-mask>

ip_addr	IP address used by the P330 to connect via its PPP interface
net-mask	Subnet mask used by the P330 to connect via its PPP interface

Example:

```
P330-N> set interface ppp 149.49.34.125 255.255.255.0
Interface ppp has its ip address set
```

Use the set interface ppp command to enter modem mode, enter terminal mode, disconnect the PPP session or to reset the connected modem.

The syntax for this command is:

set interface ppp {enable|enable-always|disable|off|reset}

enable	Enable PPP and enter modem mode.
enable-always	Enable automatic reentry into modem mode after modem cable disconnection or reconnection.
disable	Disable PPP and enter terminal mode
off	Disconnect the active PPP session.
reset	Reset the connected modem.

Example:

```
P330-N> set interface ppp reset
PPP has reset the connected modem.

P330-N# set interface ppp enable
Entering the Modem mode within 60 seconds...
Please check that the proprietary modem cable is plugged into
the console port

P330-N# set interface ppp disable
Entering the Terminal mode immediately
```

Set port level Command

Use the `set port level` command to set the priority level of a port. Untagged (without an 802.1p priority header) packets travelling through ports set with priority 0-3 will be served only *after* packets traveling through ports set with priority 4-7 in case of congestion. Packets arriving with an 802.1p priority header will not be modified by this command.

The syntax for this command is:

`set port level` `<mod_num>/<port_num> {value}`

value	Priority level (0-7)

Example:

To set the priority level for port 2 on module 1 to 7:

```
P330-N# set port level 1/2 7
Port 1/2 port level set to 7
```

Set port negotiation Command

Use the `set port negotiation` command to enable or disable autonegotiation on a port. If autonegotiation is disabled, you can set port parameters using the relevant CLI commands. If autonegotiation is enabled, these commands have no effect. For Fiber Gigbit Ethernet ports it can determine the flow control (pause) mode only.

The syntax for this command is:

`set port negotiation` `<mod_num>/<port_num> {enable|disable}`

Example:

To disable autonegotiation on port 1, module 4:

```
P330-N# set port negotiation 4/1 disable
Link negotiation protocol disabled on port 4/1.
```

Set port enable Command

Use the `set port enable` command to enable a port or a range of ports.

The syntax for this command is:

`set port enable` [mod_num/port_num]

mod _num	The module number
port_num	The port number

Example:

To enable port 3 on module 2:

```
P330-N# set port enable 2/3
Port 2/3 enabled.
```

Set port disable Command

Use the `set port disable` command to disable a port.

The syntax for this command is:

`set port disable` <mod_num>/<port_num>

Example:

```
P330-N# set port disable 5/10
Port 5/10 disabled.
```

Set port speed Command

Use the `set port speed` command to configure the speed of a 10/100Base-T port. If autonegotiation mode is enabled for such ports, the port's speed is determined by autonegotiation, and an error message is thus generated if you attempt to perform the `set port speed` command in this case.

The syntax for this command is:

`set port speed` <mod_num>/<port_num> {value}

Example:

To configure port 2 on module 2 port speed to 10 Mbps:

```
P330-N# set port speed 2/2 10MB
Port 2/2 speed set to 10 Mbps.
```

Note: This command is not supported for P332G-ML and P332GT-ML ports. An error message is generated if you attempt to perform the `set port speed` command for P332G-ML and P332GT-ML ports.

Set port duplex Command

Use the `set port duplex` command to configure the duplex mode of a 10/100Base-T port. You can configure the duplex mode to either Half or Full duplex. If autonegotiation mode is enabled for such ports, the port's duplex mode is determined by autonegotiation, and an error message is thus generated if you attempt to perform the `set port duplex` command in this case.

Note: P332G-ML and P332GT-ML module ports work in Full duplex mode only.

The syntax for this command is:

`set port duplex` `<mod_num>/<port_num> {full|half}`

Example:

To set port 1 on module 2 to full duplex:

```
P330-N# set port duplex 2/1 full
Port 2/1 set to full-duplex.
```

Set port name Command

Use the `set port` name to configure a name for a port. If you do not specify a name, the port name remains empty.

The syntax for this command is:

`set port name` `<mod_num>/<port_num> [<name>]`

name	Name assigned to the port.

Example:

```
P330-N# set port name 1/2 arthur

Port 1/2 name set.
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set port trap Command

Use the `set port trap` command to enable / disable generic SNMP uplink / downlink traps from a port.

The syntax for this command is:

`set port trap` `<mod_num>/<port_num> {enable|disable}`

Example:

```
P330-N# set port trap 1/2 enable
Port 1/2 up/down trap enabled.
```

Set port vlan Command

Use the `set port vlan` command to set the Port's VLAN ID (PVID). The VLAN number must be within the range 1 to 3071.

The syntax for this command is:

`set port vlan` `<value> <mod_num>/<port_num>`

value	Number between 1 and 3071, identifying the VLAN.
mod_num / port_num	The module number / the port number.

Example:

To set VLAN 850 to include ports 4 through 7 on module 3.

```
P330-N# set port vlan 850 3/4-7
VLAN 850 modified.
VLAN  Mod/Ports
---- ----------------------
850   3/4-7
```

Set port vlan-binding-mode Command

Use the set port vlan-binding-mode command to define the binding method used by ports.

The syntax for this command is:

```
set port vlan-binding-mode [port_list] [value]
```

port list	module and ports to bundle (format: module / port)
value	**static** - the port supports only the VLAN as configured per port **bind-to-configured** - the port supports the VLANs configured on the device **bind-to-all** - the port support the whole range of VLANs on the device

Example:

```
P330-N# set port vlan-binding-mode 1/5-9 static
Set Port vlan binding method:1/5
Set Port vlan binding method:1/6
.
.
```

Set port static-vlan Command

Use the set port static-vlan command to statically assign VLANs to ports.

The syntax for this command is:

`set port static-vlan` `[module/port range] [vlan num]`

`[module/port]` - port range

`{vlan range]` - vlan to bind to port

Example:

```
P330-N# set port static-vlan 1/4-6 9
```

Set port channel Command

Use the `set port channel` command to enable or disable a Link Aggregation Group (LAG) interface on the module. LAG creation requires a LAG name to be specified. There is no default name.

You can also add or remove a port from an existing LAG. All ports in the LAG are configured with the parameters of the first port that is added to the LAG. These parameters include port administrative status, speed, duplex, autonegociation mode, VLAN ID, tagging mode, binding mode, and priority level. When adding a port to an existing LAG, type the same LAG-name, otherwise you will create a new LAG. The added port must belong to the same LAG group - refer to the “LAG” marking on device’s front panel.

The syntax for this command is:

```
set port channel [port_list] [value] [name]
```

port_list	module and ports to bundle (format: module / port)
value	on / off to enable / disable a channel for the specified module ports
name	channel name

```
P330-1(super)# set port channel 1/1-3 on test
Port 1/1 channel mode set to on
Port 1/2 was added to channel
Port 1/3 was added to channel
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set port classification Command

Use the `set port classification` command to set the port classification to either regular or valuable. Any change in the Spanning Tree state from Forwarding for a valuable port will erase all learnt MAC addresses in the stack.

The syntax for this command is:

```
set port classification [module/port]  {regular | valuable}
```

module port	module / port range

regular | valuable	port classification

Example:

```
P330-1(super)# set port classification 2/19 valuable
Port 2/19 classification has been changed.
```

Set port redundancy on/off Command

Use the `set port redundancy` command to define/remove redundancy schemes between a Primary and a Secondary link. The link can be any port that does not belong to a LAG, or a LAG interface. In either case, there should not be any redundancy scheme already defined on any of the links.

The syntax for this command is:

`set port redundancy` `<mod_num>/<prim_port_num> <mod_num>/ <second_port_num> {on/off} [<redundancy_name>]`

prim_port_num	Primary link of the redundancy scheme
second_port_num	Secondary link of the redundancy scheme
redundancy_name	Name for the redundancy scheme (optional)

Example:

```
P330-N# set port redundancy 1/7 2/12 on red1
uplink: Port 2/12 is redundant to port 1/7.

Port redundancy is active - entry is effective immediately
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set port redundancy Commands

Use the `set port redundancy` commands to enable or disable the defined redundancy schemes. Using this command will not delete existing redundancy entries. A port redundancy scheme is removed once a module is removed from the stack.

Note: You must disable Spanning Tree before you can enable redundancy.

The syntax for this command is:

set port redundancy {enable|disable}

Example:

```
P330-N# set port redundancy enable
All redundancy schemes are now enabled
```

Set internal buffering Command

The `set internal buffering` command allows you to set the size (either Maximum or Minimum) of the Receive (Rx) buffer allocated to each port of the specified module. This command is meaningless when any port of the module is operating with flow control ON.

The syntax for this command is:

set internal buffering <mod_num> {max|med|min}

max	Sets the internal receive buffer to its maximum size.
med	Sets the internal receive buffer capacity dynamically
min	Sets the internal receive buffer to its minimum size (this is the Default).

Example:

```
P330-N> set internal buffering 1 max
Done.
```

Note: This command is not supported P332G-ML and P332GT-ML modules and should be used only for the other P330 modules in the stack .

Set boot bank Command

Use the `set boot bank` command to configure the software bank from which the module will boot at the next boot process. This command should be issued separately for each module in the stack using the `session` command.

Note: This command is not supported by the P333R and P333R-LB switches.

The syntax for this command is:

```
set boot bank <value>
```

value {bank-a | bank-b}

Example:

```
P330-1(super)# set boot bank bank-a

Boot bank set to bank-a
```

Set intermodule port redundancy Command

Use the `set intermodule port redundancy` command to define or delete the stack's unique intermodule redundancy scheme. The defined scheme can be enabled or disabled using the reversed `set port spantree enable/disable` command.

The syntax for this command is:

`set intermodule port redundancy` `<module/prim-port> <module/second-port> {on [<name>]}`

<module/prim-port>	The primary port number
<module/second-port>	The secondary port number
{on}	Set the intermodule redundancy
[<name>]	The name of the fast redundancy (default is 'fast')

Example:

```
P330-N> set intermodule port redundancy 1/7 2/12 on backbone
backbone: port 2/12 is intermodule redundant to port 1/7
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set intermodule port redundancy off Command

Use the `set intermodule port redundancy off` command to clear the intermodule redundancy.

The syntax for this command is:

`set intermodule port redundancy off`

Set port mirror Command

Use the `set port mirror` command to define a port mirroring source-destination pair in the stack.

The syntax for this command is:

`set port mirror source-port` <mod_num>/<port_num> **`mirror-port`** <mod_num>/<port_num> **`sampling`** {always|disable} **`direction`** {rx|tx|both}

always	Keyword to activate the port mirroring entry
disable	Keyword to change the status of the port mirroring entry to “not active”
rx	Keyword to copy only incoming traffic
tx	Keyword to copy only outgoing traffic
both	Keyword to copy both incoming and outgoing traffic

Example:

```
P330-N# set port mirror source-port 1/9 mirror-port 1/10
sampling always direction both
Mirroring both Rx and Tx packets from port 1/9 to port 1/10 is
enabled
```

Set port spantree

Use the `set port spantree` command to enable or disable the spanning tree mode for specific switch ports.

The syntax for this command is:

```
set port spantree {enable|disable} [module/port]
```

enable | disable	Enables or disables the spanning tree mode for the specified ports.
module / port	The module / port number.

Example:

Enable the spanning tree mode for port 2 on module 3.

```
P330-N# set port spantree enable 3/2
```

Set port spantree priority Command

Use the `set port spantree priority` command to set the priority level of a port. This value defines the priority of a port to be blocked in case two ports with the same costs cause a loop.

The syntax for this command is:

```
set port spantree priority [module/port] [value]
```

module / port	The module number / the port number.
value	Number representing the priority of the port. The priority level is from 0 to 255, with 0 indicating high priority and 255 indicating low priority.

Set port spantree cost Command

Use the `set port spantree cost` command to set the cost of a port. This value defines which port will be allowed to forward traffic if two ports with different costs cause a loop.

The syntax for this command is:

```
set port spantree cost [module/port] [value]
```

module / port	The module number / the port number.
value	Number representing the cost.

Set port security Command

Use the `set port security` command to enable MAC security on a port, a range of ports, a module, or a stack.

The syntax for this command is:

`set port security` `{ enable | disable } [<module>[/<port>]]`

`{ enable | disable }` - set the port security enable or disable

`[<module>[/<port>]]` - set specific module / port

Example:

```
P330-N> set port security enable 1/2
Port 1/2 secured.
```

Note: This command is not supported in P332G-ML and P332GT-ML modules. This command is used to set post security for ports in other P330 modules in the stack.

Set cascading Command

Use the `set cascading` command to enable or disable fault-trap sending for unconnected cascading links. The default setting is disable.

The syntax for this command is:

`set cascading``{up|down}`**`fault-monitoring`** `{enable|disable}<mod-num>`

Example:

```
P330-N# set cascading down fault-monitoring enable 1
Module 1 cascading-down fault monitoring enabled.
```

Set inband vlan Command

Use the `set inband vlan` command to set a value for the management vlan (from 1 to 3071).

The syntax for this command is:

`set inband vlan` `<value>`

`value`	A VLAN number between 1 and 3071.

Example:

```
P330-N# set inband vlan 1
```

```
Management VLAN number set to 1
```

Set vlan Command

Use the set vlan command to create vlans.

The syntax for this command is:

set vlan <vlan-id> [name <vlan-name>]

vlan-id	vlan number
vlan-name	vlan name

Example:

```
P330-N# set vlan 3 name v3
VLAN ID 3 is named v3.
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set port flowcontrol Command

Use the `set port flowcontrol` command to set the send / receive mode for flow-control frames (IEEE 802.3x or proprietary) for a full duplex port. Each direction (send or receive) can be configured separately only for Gigabit Ethernet ports. Proprietary flow control cannot be configured on Gigabit ports. The `set flowcontrol` command cannot be used on Gigabit ports for which autonegotiation is enabled.

The syntax for this command is:

```
set flowcontrol [direction] [module/port] [value]
```

direction	• receive / send / all
module / port	• module / port number
value	• on / off / proprietary

Example:

```
P330-1(super)# set port flowcontrol all 2/20 on
Port 2/20 flow control administration status set to on
```

Set port auto-negotiation-flowcontrol-advertisement Command

The `set port auto-negotiation-flowcontrol-advertisement` command sets the flowcontrol advertisement for a Gigabit port when performing autonegotiation.

The syntax for this command is:

`set port auto-negotiation-flowcontrol-advertisement` `<mod_num>/<port_num> {no-flowcontrol|asym-tx-only|sym-only|sym-and-asym-rx}`

no-flowcontrol	The port will advertise no pause capabilities
asym-tx-only	The port will advertise asymmetric Tx pause capabilities only
sym-only	The port will advertise symmetric pause capabilities only
sym-and-asym-rx	The port will advertise both symmetric and asymmetric Rx pause capabilities

Example:

```
P330-N#  set port auto-negotiation-flowcontrol-advertisement
1/5 asym-tx-only


P330-N# Port 1/5 pause capabilities was set
```

Set trunk Command

Use the `set trunk` command to configure the tagging mode of a post.

`set trunk` `[module/port] [value]`

module/port	module/port number
value	off/dot1q

Example:

```
P330-1(super)# set trunk 2/20 dot1q
Dot1Q VLAN tagging set on port 2/20.
```

Set spantree Commands

Use the `set spantree` command to enable/disable the spanning-tree protocol for the stack.

Note: When you disable STP, blocking ports are disabled in order to prevent loops in the network. As a result, you *should* wait 30 seconds before disabling STP if you reset the switch, enabled STP, or inserted a new station.

The syntax for this command is:

set spantree {enable|disable}

Example:

```
P330-N# set spantree enable
bridge spanning tree enabled.
```

Set spantree priority Command

Use the `set spantree priority` command to set the bridge priority for STP.

The syntax for this command is:

set spantree priority <priority>

priority	Number representing the priority level from 0 to 65535, with 0 indicating high priority and 65535 indicating low priority.

Example:

This example shows how to set the priority to 45000:

```
P330-N# set spantree priority 45000
Priority enabled
```

Set autopartition Command

Use the `set autopartition` command to enable or disable auto-partitioning on specific modules of the stack.

The syntax for this command is:

set autopartition <enable|disable>[module]

Example:

```
P330-N# set autopartition enable 3
Auto-partition is enabled in module 3.
```

Note: This command is not supported in P332G-ML and P332GT-ML modules. This command is used to set the autopartition status for the other P330 modules in the stack.

Set license Command

The `set license` command enables you to activate the SMON / routing capability of the Avaya P330 stack. An Avaya P330 stack can include several Avaya P330 modules. One SMON / routing license is required per Avaya P330 stack.

For a full description of the SMON / routing License and the installation procedure please refer to the Installation Guide provided with the SMON / routing License.

The syntax for this command is:

`set license` `[module] [license] [featureName]`

module	The module number.
license	The license number.
featureName	The name of the feature, either `smon` or `routing`.

Example:

```
P330-N> set license 1 021 1ad bad ca5 8d2 ccd smon
```

Set ppp authentication incoming Command

Use the `set ppp authentication incoming` command to define the authentication method used for a PPP server or client session.

The syntax for this command is:

`set ppp authentication incoming` `{pap|chap|none}`

pap	PAP authentication method
chap	CHAP authentication method
none	No authentication

Example:

```
P330-N(super)# set ppp authentication incoming chap
```

Set ppp incoming timeout Command

Use the `set ppp incoming timeout` command to configure the number of minutes until the system automatically disconnects an idle PPP incoming session.

The syntax for this command is:

`set ppp incoming timeout` `<timeout>`

`timeout` The timeout in minutes.

Example:

```
P330-N> set ppp incoming timeout 15
PPP incoming session will automatically disconnect after 15
minutes of idle time
```

Set ppp baud-rate Command

Use the set ppp baud-rate command to define the baud rate used in PPP sessions. Note that the peer baud rate must be set at the same value as the host.

The syntax for this command is:

`set ppp baud-rate` `<9600 | 19200 | 38400>`

Example:

```
P330-N# set ppp baud-rate 38400
```

Set web aux-files-url Command

Use the `set web aux-files-url` command to allow the Device Manager to automatically locate the URL (the http: / / www address and path) of the Web server containing the Device Manager help files and Java plug-in.

Note: Ensure that the Web server is always accessible otherwise Web access to the device may take a few minutes.

The syntax for this command is:

`set web aux-files-url` `<//IP address/directory name>`

Example:

```
P330-N# set web aux-files-url //192.168.47.25/emweb-aux-files
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Set intelligent-multicast Command

Use the `set intelligent-multicast` command to enable or disable the IP-multicast filtering application.

The syntax for this command is:

`set intelligent-multicast` {enable|disable}

Example:

```
P330-N> set intelligent-multicast enable
Done!
```

Set intelligent-multicast client port pruning time Command

Use the `set intelligent-multicast client-port-pruning time` command to define aging time for client ports.

The syntax for this command is:

`set intelligent-multicast client-port-pruning time` <time>

`time` time in seconds

Example:

```
P330-N> set intelligent-multicast client-port-pruning-time 20
Done!
```

Set intelligent-multicast router port pruning time Command

Use the `set intelligent-multicast router-port-pruning time` command to define aging time for router ports.

The syntax for this command is:

`set intelligent-multicast router-port-pruning time` <time>

`time` time in seconds

Example:

```
P330-N> set intelligent-multicast router-port-pruning time 20
Done!
```

Set intelligent-multicast group filtering delay time Command

Use the `set intelligent-multicast group-filtering-delay time` command to define group filtering time delays.

The syntax for this command is:

`set intelligent-multicast group-filtering-delay time` `<time>`

`time` time in seconds

Example:

```
P330-N> set intelligent-multicast group-filtering-delay time
20
Done!
```

Set security mode Command

Use the `set security mode` command to enable or disable MAC security at the stack level. When enabled, the ports are secured based on their individual configuration. When disabled, all the ports in a stack are non-secured.

The syntax for this command is:

`set security mode` `{ enable | disable }`

Example:

```
P330-N> set security mode enable
Security mode enabled.
```

Note: The `set security mode` command does not apply to the P332G-ML and P332GT-ML, and relates only to the other P330 modules in the stack.

Set arp-aging-interval Command

Use this command to set the arp aging interval. The MAC value for the default gateway of ML agent in the ARP table, is deleted at the end of every aging interval. The default value is 10 minutes.

The syntax for this command is:

`set arp-aging-interval` `<value>`

`<value>` - interval (minutes)

Example:

```
P330-N# set arp-aging-interval 20
ARP aging interval was set to 20 minutes.
```

Set arp-tx-interval Command

Use the set arp-tx-interval command to set the keep-alive frames sending interval. Setting the interval to 0 disables the transmission of the keep-alive frames.

The syntax for this command is:

`set arp-tx-interval` `<value>`

`<value>` - interval (seconds)

Example:

```
P330-N# set arp-tx-interval 15
ARP tx interval was set to 15 seconds.
```

set welcome message

Use the `set welcome message` command to set a welcome message to appear after a reboot or after opening a new session (see `session` command) in the stack.

The syntax for this command is:

`set welcome message` `[string]`

string	**string -** The string to be used as the welcome message. **blank -** Restores the default string.

Output Example:

```
P330-N# set welcome message avaya
The new welcome string is “avaya”
```

Note: If you wish to define a string which includes spaces, you must enclose the entire string in quotation marks, e.g. "new york".

Sync time Command

This command synchronizes the time used by all modules in a stack.

The syntax for this command is:

sync time

Example:

```
P330-N# sync time
Time has been distributed.
```

Get time Command

This command retrieves the time from the network.

The syntax for this command is:

get time

Example:

```
P330-N# get time
Time is already being acquired from network!
```

Reset Command

Use the `reset` command to restart the system or an individual module. If no module number is defined or the module number of the Master is defined, the command resets the entire system. If the module number is defined, the command resets the specified module only.

The syntax for this command is:

reset [<mod_num>]

Example:

To reset the Master agent and force the entire system to reset:

```
P330-N# reset
This command will force a switch-over to the master module and
disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
```

To reset module 4:

```
P330-N# reset 4
This command will reset module 4 and may disconnect your
telnet session.
Do you want to continue (y/n) [n]? y
```

```
Resetting module 4...
```

Nvram initialize Command

Use the `nvram initialize` command to reset the P330 parameters to the factory defaults. If no options are specified for this command, only the Layer 2 parameters will be reset.

The syntax for this command is:

`nvram initialize` `[switch|all]`

switch	Resets all the switching level parameters (Layer 2 only) throughout the stack
all	Resets all parameters including licenses and routing parameters of the Layer 3 modules present in the stack

Example:

```
P330-N# nvram initialize
This command will force a factory default and switch-over to
the master module and disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
host%
```

Configure Command

The `configure` command is not used in the Layer 2 CLI. It is used with the Layer 3 CLI. Use the configure command to enter Configure Mode (See Security Levels on page 220).

Rmon history Command

Use the `rmon history` command to create an RMON history entry.

The syntax for this command is:

`rmon history` `<history index> [<module>[</port>]]` **`interval`** `<interval>` **`buckets`** `<number of buckets>` **`owner`** `<owner name>`

history_index	This is the history index number of this entry (it is advisable to use the same interface number as your history index number)
module / port	The module number / the port numbe.r

interval	The interval between 2 samples.
number of buckets	The number of buckets defined
owner name	Owner name string

Example:

```
P330-N# rmon history 1026 1026 3/2 30 buckets 20 owner amir
history 1026 was created successfully
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Rmon alarm Command

Use the `rmon alarm` command to create a new RMON alarm entry.

The syntax for this command is:

`rmon alarm` `<Alarm Number> <variable> <interval> <sampletype>` **`rising-threshold`** `<rising threshold> <rising event>` **`falling-threshold`** `<falling threshold> <falling event> <startup alarm> <owner>`

alarm number	This is the alarm index number of this entry (it is advisable to use the same interface number as your alarm index number.)
variable	This is the MIB variable which will be sampled by the alarm entry.
interval	The interval between 2 samples
sample type	This can be set to either **delta** (the difference between 2 samples) or an **absolute** value.
rising threshold	This sets the upper threshold for the alarm entry.
rising event	The RMON event entry that will be notified if the upper threshold is passed.
falling threshold	This sets the lower threshold for the alarm entry.

falling event	The RMON event entry that will be notified if the lower threshold is passed.
startup alarm	The instances in which the alarm will be activated. The possible parameters are: **Rising, Falling, risingOrfalling.**
owner	Owner name string

Example:

```
P330-N# rmon alarm 1026 1.3.6.1.2.1.16.1.1.1.5.1026 60 delta
rising-threshold 10000 1054 falling-threshold 10 1054
risingOrFalling amir
alarm 1026 was created successfully
```

Rmon event Command

Use the `rmon event` command to create an RMON event entry.

The syntax for this command is:

`rmon event` `<Event Number> <type>` **`description`** `<description>` **`owner`** `<owner>`

event number	This is the event index number of this entry.
type	The type of the event. The possible parameters are: **trap, log, logAndTrap, none.**
description	A user description of this event
owner	Owner name string

Example:

```
P330-N#  rmon event 1054 logAndTrap description "event for
monitoring amir's computer" owner amir
event 1054 was created successfully
```

Copy stack-config tftp Command

Use the `copy stack-config tftp` command to upload the stack-level parameters from the current NVRAM running configuration into a file via TFTP.

Note: Create the file into which you wish to upload the stack-level parameters prior to executing this command.

The syntax for this command is:

copy stack-config tftp <filename> <ip>

filename	file name (full path)
ip	The ip address of the TFTP server

Example:

```
P330-N# copy stack-config tftp c:\conf.cfg 192.168.49.10
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'upload status' command
*********************************************************************
* If you are currently running the P330 Device Manager application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                              *
*********************************************************************
```

Copy module-config tftp Command

Use the `copy module-config tftp` command to upload the module-level parameters from the current NVRAM running configuration into a file via TFTP.

If an error occurred during upload (you can check this using the command `show tftp upload status`) you must fix the problem. The following is a list of possible problems:

a You did not create an empty text file at the destination server (0 Bytes).
b You do not have the correct path to the file.
c The destination server is not active / on.
d The destination server is unreachable.

Then, perform the upload procedure again *twice* as follows:

a Delete the destination file and recreate a correctly named empty file at the destination server (0 Bytes)
b Type the command `copy module-config tftp` for the first time.
c Delete the destination file and recreate a correctly named empty file at the destination server (0 Bytes)
d Type the command `copy module-config tftp` again, a second time.

The syntax for this command is:

copy module-config tftp <filename> <ip> <mod_num>

filename	file name (full path)
ip	The ip address of the TFTP server
mod-num	The module number

Example:

```
P330-N# copy module-config tftp c:\p332ml\switch1.cfg
192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show tftp upload status' command

**********************************************************************
* If you are currently running the P330 Device Manager application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                               *
**********************************************************************
```

Copy tftp stack-config Command

Use the `copy tftp stack-config` command to download the stack-level configuration from a saved file into the current NVRAM running configuration, via TFTP. To use this command, you need to have an active tftp server, and to create a file into which to download the data. If Avaya Multi-Service Network Manager is running, an additional tftp server is not required.

Note: You should perform the `nvram initialize` command prior to the `copy tftp` operation.

The syntax for this command is:

copy tftp stack-config <filename> <ip>

filename	file name (full path)
ip	The ip address of the TFTP server

Example:

```
P330-N# copy tftp stack-config c:\p332ml\switch1.cfg
192.168.49.10
```

Copy tftp module-config Command

Use the `copy tftp module-config` command to download the module-level configuration from a saved file into the current NVRAM running configuration of a module, via TFTP. To use this command, you need to have an active tftp server, and to create a file into which to download the data. If Avaya Multi-Service Network Manager is running, an additional tftp server is not required.

Note: You should perform the `nvram initialize` command prior to the `copy tftp` operation.

The syntax for this command is:

`copy tftp module-config` `<filename> <ip> <mod_num>`

filename	File name (full path)
ip	The ip address of the TFTP server

Example:

```
P330-N# copy tftp startup-config  c:\p332ml\switch1.cfg
192.168.49.10 5
```

Copy tftp EW_archive Command

Use the `copy tftp EW_archive` command to download the P330 Device Manager application into the module via TFTP. To use this command, you need to have an active tftp server, and to create a file into which to download the data. If Avaya Multi-Service Network Manager is running, an additional tftp server is not required.

The syntax for this command is:

`copy tftp EW_archive` `<filename> <ip> <mod_num>`

filename	Embedded Web Manager image file name (full path)
ip	The ip address of the TFTP server
mod_num	Target module number

Example:

```
P330-N# copy tftp EW_archive c:\p332ml\p332mlweb201
192.168.49.10 5
```

Copy tftp SW_image Command

Use the `copy tftp SW_image` command to update the software image and the device manager applications of a designated module. To use this command, you need to have an active tftp server, and to create a file into which to download the data. If Avaya Multi-Service Network Manager is running, an additional tftp server is not required.

The syntax for this command is:

copy tftp SW_image <image-file> **EW_archive <**filename**>**<ip> <mod_num>

image-file	Common name for the files that contain the Software Image and Embedded Web archive (full path)
filename	Embedded Web Manager image file name (full path)
ip	The ip address of the TFTP server
mod_num	Target module number

Example:

```
P330-N# copy tftp SW_image c:\p332ml\p332mlweb101 EW_archive
c:\p332ml\p332mlweb201 192.168.49.10 5
P330-N#
```

Radius Commands

The following radius commands are accessible from Privileged mode.

Set radius authentication secret Command

Use the `set radius authentication secret` command to enable secret authentication for the P330 unit.

The syntax for this command is:

`set radius authentication secret <string>`

`string` text password

Example:

```
P330-N(super)# set radius authentication secret sodot
P330-N(super)#
```

Set radius authentication server Command

Use the `set radius authentication server` command to set a primary or secondary RADIUS server IP address.

The syntax for this command is:

`set radius authentication server` `<ip-address> <primary|secondary>`

ip-addr	IP address of the RADIUS authentication server
primary	default - Primary authentication server
secondary	Secondary authentication server

Example:

```
P330-N(super)# set radius authentication server 192.168.38.12
primary
```

Clear radius authentication server Command

Use the `clear radius authentication server` command to remove a primary or secondary RADIUS authentication server.

The syntax for this command is:

`clear radius authentication server``[{primary|secondary}]`

Set radius authentication retry-time Command

Use the `set radius authentication retry-time` command to set the time to wait before re-sending an access request.

The syntax for this command is:

`set radius authentication retry time` `<time>`

`time` retry time in seconds

Set radius authentication retry-number Command

Use the `set radius authentication retry-number` command to set the number of times an access request is sent when there is no response.

The syntax for this command is:

`set radius authentication retry number` `<number>`

`number` retry number

Set radius authentication udp-port Command

Use the `set radius authentication udp-port` command to set the RFC 2138 approved UDP port number. Normally, the UDP port number should be set to its default value of 1812. Some early implementations of the RADIUS server used port number 1645.

The syntax for this command is:

`set radius authentication server udp-port` `<number>`

Supervisor Level Commands

This level includes all the commands of the User and Privileged Levels (including all `show` and `set` commands).

Username Command

Use the `username` command to add a local user account. You can only do this from within the Supervisor Level.

The syntax for this command is:

`username` `<name>` **`password`** `<passwd> access-type{read-only|read-write|admin}`

name	New user name
passwd	user's password
access-type	Access type definition - read only, read-write or administrator.

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

No username Command

Use the `no username` command to remove a local user account.

The syntax for this command is:

`no username` `<name>`

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Show username Command

Use the show username command to display the username.

The syntax for this command is:

show username

Example:

```
P330-N> show username
User account            password               access-type
--------------  ------------------------------  -----------
root                  root                          admin
```

Set ppp chap-secret Command

Use the `set ppp chap-secret` command to configure the shared secret used in PPP sessions with CHAP authentication.

The syntax for this command is:

set ppp chap-secret <chap-secret>

chap-secret The shared secret, 4 to 32 characters.

Example:

```
P330-N(super)# set ppp chap secret sodot
PPP shared secret for CHAP authentication is set
```

Show radius authentication Command

Use the `show radius authentication` command to display all RADIUS authentication configurations. The shared secrets are not displayed.

The syntax for this command is:

show radius authentication

Example:

```
P330-N(super)# show radius authentication
RADIUS authentication parameters:
---------------------------------
Mode:                 Enabled
Primary-server:       192.168.42.252
Secondary-server:     192.168.48.134
Retry-number:         4
Retry-time:           5
UDP-port:             1645
Shared-secret:        sodot
```

Set radius authentication Command

Use the `set radius authentication` command to enable or disable authentication for the P330 unit. RADIUS authentication is disabled by default.

The syntax for this command is:

`set radius authentication` `[enable|disable]`

Tech Command

Use the `tech` command to enter tech mode. This command is reserved for service personnel use only.

CLI – Layer 3

This chapter provides all the Layer 3 CLI commands, parameters and their default values. Not all groups, parameters and commands are available when the P330 boots up from its INIT software.

Before you attempt to access Layer 3 CLI commands, review the Obtaining and Activating a License Key procedures on page 40, and P330 Sessions on page 220.

Router Configuration Contexts

At this point you can either use the general P330 commands available from the `Router(configure)# prompt` or you can enter one of two router configuration context modes:

- Router interface context:
  This allows you to define parameters individually for each interface. To enter this context, type **`interface <interface_name>`**
  The prompt changes to **`Router>(config-if:<interface_name>)#`**
- Router protocol context:
  This allows you to define parameters for a specific routing protocol (RIP, OSPF, VRRP, and SRRP). To enter this context, type **`router <protocol_name>`**
  The prompt changes to **`Router>(configure router:protocol_name)#`**

To exit these context modes, type the command **`exit`**.

How Commands are Organized

Command descriptions are organized into the following groups:

The commands in each group are sub-divided into the following command mode sub-groups.

- User / Privileged — User / Privileged Mode Commands
- Configure — Configure Mode Commands
- Interface — Interface Context Mode Commands
- Router — Router Context Mode Commands

The commands in every group are summarized in a Table at the beginning of each Section.

System Commands

Table 6.1 System Commands

User /Privileged Command Mode

hostname Command

Use the `hostname` command to change the system prompt used for the router. This command does not change the system prompt of the stack. To change the system prompt of the stack, use the host name command in the switch CLI tree.

The syntax for this command is:

`[no] hostname` `[<hostname_string>]`

`hostname_string`	The string to be used as the hostname (up to 20 characters).

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

show device-mode Command

Use the `show device-mode` command to show the P332-ML operating mode you are currently in. Possible modes are Router, or Switch.

The syntax for this command is:

`show device-mode`

show copy status Command

Use the `show copy status` command to show the status of the local configuration copy operation.

The syntax for this command is:

`show copy status`

show tftp download status Command

Use the `show tftp download status` command to view the status of the tftp download operation.

The syntax for this command is:

`show tftp download status`

show tftp upload status Command

Use the `show tftp upload status` command to view the status of the tftp upload operation.

The syntax for this command is:

`show tftp-upload status`

show erase status Command

Use the `show erase status` command to view the status of the erase configuration operation.

The syntax for this command is:

`show erase status`

show running-config Command

Use the `show running-config` command to show configuration currently running on the switch.

The syntax for this command is:

`show running-config`

show startup-config Command

Use the `show startup-config` command to show configuration loaded at startup.

The syntax for this command is:

`show startup-config`

show system Command

Use the `show system` command to show the P332-ML system parameters.

The syntax for this command is:

`show system`

set device-mode Command

Use the `device-mode` command to change the Basic Mode of Operation of the P332-ML Module between Router and Layer 2 modes.

The syntax for this command is:

`set device-mode` `<mode>`

mode	Router | Layer2

set system contact Command

The syntax for this command is:

`set system contact` `[contact string]`

Example:

```
set system contact "Gabby ext.545"
```

set system name Command

The syntax for this command is:

`set system name` `[name string]`

Example:

```
Router-N> set system name "Banking System"
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

set system location Command

The syntax for this command is:

`set system location` `[location string]`

Example:

```
Router-N> set system location "Floor 5,Room 12"
```

copy tftp startup-config Command

Use the `copy tftp startup-config` command to copy the P332-ML configuration from the saved TFTP file to the Startup Configuration NVRAM.

The syntax for this command is:

`copy tftp startup-config` `<filename> <ip>`

filename	file name (full path)
ip	The ip address of the host

Example:

```
copy tftp startup-config  c:\p332\router1.cfg 192.168.49.10
```

copy running-config tftp Command

Use the `copy running-config tftp` command to copy the P332-ML configuration from the current VRAM Running Configuration to the TFTP file.

The syntax for this command is:

`copy running-config tftp` `<filename> <ip>`

filename	file name (full path)
ip	The ip address of the host

Example:

```
Router-N> copy running-config tftp c:\p332\router1.cfg
192.168.49.10
```

copy running-config startup-config Command

Use the `copy running-config startup-config` command to copy the P332-ML configuration from the current VRAM Running Configuration to the Startup Configuration NVRAM.

The syntax for this command is:

`copy running-config startup-config`

copy startup-config tftp Command

Use the `copy startup-config tftp` command to copy the P332-ML configuration from the NVRAM Startup Configuration to the TFTP file.

The syntax for this command is:

`copy startup-config tftp` `<filename> <ip>`

filename	file name (full path)
ip	The ip address of the host

Example:

```
Router-N> copy startup-config tftp c:\p332\router1.cfg
192.168.49.10
```

erase startup-config Command

The `erase startup-config` command erases the P332-ML module NVRAM configuration.

The syntax for this command is:

`erase startup-config`

reset Command

The `reset` command resets the P332-NL module. This command resets only the specific module. If the module is the master of the stack the entire stack is reset.

If you want to keep changes you made to the current running configuration use the `copy running-config startup-config` command first.

The syntax for this command is:

`reset`

ping Command

Use the `ping` command to check host reachability and network connectivity.

The syntax for this command is:

`ping` `<host> [<packetsize> [<interval>]]`

host	IP address of the target system.
packetsize	An integer, the size of the packet sent during a ping operation. The default is 56 bytes.
interval	An integer, the number of seconds between successive ping messages. The default is 1 second.

Example:

```
Router-N> ping 149.49.50.13 5 8
```

Example:

```
Router-N> ping 149.49.50.13
```

traceroute Command

Use the `traceroute` command as a trace route utility.

The syntax for this command is:

`traceroute` `<host>`

host	IP address.

Example:

```
Router-N> traceroute 192.168.50.13
```

session Command

See Session Command on page 44.

IP Commands

Table 6.2 IP Commands

Table 6.2 IP Commands

User Mode

show ip route Command

Use the `show ip route` command to display information about the IP unicast routing table.

The syntax for this command is:

`show ip route` `[<ip-address>[<ip-mask>]`

ip-address	The IP address of the routes
ip-mask	The ip mask of the routes.

Example:

```
show ip route                                Display all routes
show ip route 137.32.50.13                   Display a single route
show ip route 137.44.50.13 255.255.255.0     Display range of routes
```

show ip route best-match Command

Use this command to display a routing table for a destination address.

The syntax for this command is:

`show ip route best-match <dst addr>`

`dst addr`	IP address

Example:

```
Router-1(super)# sh ip route best-match 199.93.0.0
Searching for: 199.93.0.0
Showing 1 rows
```

```
Network          Mask        Interface      Next-Hop     Cost  TTL  Source
-------------- -------------- ----------- -------------- ----- --- -----
199.93.0.0     255.255.0.0     e-135new     135.64.76.1         1 n/a STAT-HI
```

show ip route static Command

Use this command to display the static routes.

The syntax for this command is:

```
show ip route static [<ip addr> [<mask>] ]
```

ip-address	The IP address of the routes
mask	The ip mask of the routes.

Example:

```
Router-1 (super)#  sh ip route static
Showing 34 rows
Network        Mask          Interface       Next-Hop     Cost Pref Active
-------------- ------------- --------------- -------------- ---- ---- ------
10.0.8.0       255.255.255.0  e-36           149.49.36.11   1   high  Yes
135.0.0.0      255.0.0.0      e-135new       135.64.76.1    1   high  Yes
135.64.0.0     255.255.0.0    e-135          135.87.164.1   1   high  No
149.49.0.0     255.255.0.0     zevel         10.10.254.253  1   low   Yes
149.49.2.0     255.255.255.0   n/a           v-Route-FW 1   1   high  Yes
```

show ip route summary

Use this command to display the number of routes known to the switch.

The syntax for this command is:

```
show ip route summary
```

Example:

```
Router-1 (super)#  sh ip route summary
IP Route Summary:
        Current number of routes: 69
```

show ip arp Command

Use the `show ip arp` command to display the Address Resolution Protocol (ARP) cache.

The syntax for this command is:

`show ip arp` `[<if-name> | <vlan> | <ip addr> | <ip-mask> static]`

if-name	Interface name (string up to 32 chars)
vlan	VLAN NAME (string up to 16 chars) or VLAN ID (number)
ip-addr	The IP address of the station(s)
ip-mask	The ip mask of the routes.
static	Display static ip ARP information.

Example:

```
show ip arp                                Display all ARP mapping
show ip arp marketing                     Display interface ARP mapping
show ip arp 192.168.49.1                   Display one host ARP mapping
show ip arp 192.168.49.1 255.255.255.0 Display range of ARP mapping
show ip arp marketing_vlan                 Display vlan ARP mapping
show ip arp static                         Display static ARP mapping
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

show ip reverse-arp Command

Use this command to display the IP address of a host, based on a known MAC address.

The syntax for this command is:

`show ip reverse-arp <mac addr> [<match len>]`

mac addr	MAC address
match len	The number of bytes in the address to match

Example:

```
Router-1 (super)#  sh ip reverse-arp 00:10:a4:98:97:e0

Showing 1 rows

Address          MAC Address           I/F         Type      TTL
---------------- ----------------- ----------- ------- --------
149.49.70.68     00:10:a4:98:97:e0   e-70       Dynamic    14355
```

show ip interface Command

Use the `show ip interface` command to display information for an IP interface.

The syntax for this command is:

`show ip interface` `[<interface-name>]|<ip-address>|<vlan>]`

interface-name	The name of the interface whose information you want to display.
ip-address	The IP address of the interface whose information you want to display.
vlan	The name or ID of the VLAN over which there are interfaces you want to display.

Output Example:

```
Showing 2 Interfaces
mgmt is administratively up
 On vlan Default
 Internet address is 10.49.54.14   , subnet mask is 255.255.255.0
 Broadcast address is 10.49.54.255
 Directed broadcast forwarding is disabled
 Proxy ARP is disabled

baba is administratively down
 On vlan v2
 Internet address is 192.168.0.14     , subnet mask is 255.255.0.0
 Broadcast address is 192.168.255.255
 Directed broadcast forwarding is disabled
 Proxy ARP is disabled
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

show ip protocols Command

Use the ip protocols command to display the IP routing protocol process parameters and statistics.

The syntax for this command is:

show ip protocols [<protocol>]

protocol	R IP | OSPF.

Example:

```
show ip protocols     -  Display all running protocols details
show ip protocols RIP -  Display RIP details
```

Output Example:

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, flushd after 300
  Redistributing: rip
  Default version control: rip version 1
    Interface                       Version   Key
  Routing for Networks:
  Routing Information Sources:
    Gateway                 Last Update
```

show ip icmp Command

Use the show ip icmp command to display the status of ICMP error messages.

The syntax for this command is:

show ip icmp

show ip unicast cache Command

Use the `show ip unicast cache` command to list the entries in the hardware unicast cache database.

The syntax for this command is:

`show ip unicast cache` `[<ip addr>]`

ip addr	IP address.

Output Example:

```
Router-N> show ip unicast cache

  Showing 6 Sessions.
  IP Address          NH MAC           NH VLAN
============    ========    =======
192.168.1.1     29.2.1.1       5
192.168.2.1     29.2.2.1       5
192.168.2.2     29.2.2.2       5
192.168.2.3     29.2.2.3       5
192.168.2.4     29.2.2.4       5
192.168.2.5     29.2.2.5       5
```

show ip unicast cache networks Command

Use the `show ip unicast cache networks` command to list a summary of networks handled by the hardware unicast cache database.

The syntax for this command is:

`show ip unicast cache networks` `[<net addr> <net mask>]`

net addr	The IP address of the network.
net mask	The mask IP address.

Example:

```
Router-N> show ip unicast cache networks

 Showing 7 rows (5 networks)

 Network          Mask Next Hop(s)     Total Hosts
 ================ ==== ================ ===========
 10.0.0.0           16 10.2.0.2                996
 71.0.0.0           16 0.0.0.0                   1
 130.0.0.0           8 192.168.0.130          1124
 190.0.0.0          24 10.2.0.2                250
                       192.168.0.130
 191.0.0.0          24 10.2.0.2                250
                       192.168.0.130
                                               -----
                                      Total: 2621
```

show ip unicast cache networks detailed Command

Use the `show unicast cache networks detailed` command to list the networks and hosts that are handled by the hardware unicast cache database.

The syntax for this command is:

`show ip unicast cache networks detailed``[<net addr> <net mask>]`

net addr	The IP address of the network.
net mask	The mask IP address.

Output Example:

```
Router-N> show ip unicast cache networks detailed 192.168.6.0
24
Showing 3 rows

Network       Mask     IP Address
============  ====  ===============
192.168.6.0   24    192.168.6.40
                    192.168.6.53
                    192.168.6.64
```

show ip unicast cache nextHop Command

Use the `show ip unicast cache nextHop` command to list the routers that are used as next-hop routers.

The syntax for this command is:

`show ip unicast cache nextHop`

Output Example:

```
Router-N> show ip unicast cache nextHop

 Showing 2 rows
 Next Hop
 ========
 192.168.4.1
 192.168.5.1
```

show ip unicast cache summary Command

Use this command to display the number of host networks and next-hops in the module's unicast cache.

The syntax for this command is:

```
show ip unicast cache summary
```

Example:

```
Router-1(super)# sh ip unicast cache summary
 Cache Summary
===============
Hosts     :     71
Networks  :     24
Next-Hops :     37
```

Configure Mode

interface Command

Use the `interface` command to create and / or enter the Interface Configuration Mode. Use the `no` form of this command to delete a specific IP interface.

The syntax for this command is:

`[no] interface` `<interface name>`

interface name	String (up to 32 characters)

Example:

```
Router-N(configure)# interface marketing
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

ip default-gateway Command

Use the `ip default-gateway` command to define a default gateway (router). The `no` form of this command removes the default gateway.

The syntax for this command is:

`[no] ip default-gateway` `<ip-address>[<cost>][<preference>]`

ip-address	The IP address of the router.
cost	The path cost. The default is 1
preference	Preference, either High or Low. Default is Low.

Example:

To define the router at address 192.168.37.1 as the default gateway.

```
Router-N(configure)# ip default-gateway 192.168.37.1
```

ip route Command

Use the `ip route` command to establish a static route. The `no` form of this command removes a static route.

The syntax for this command is:

`[no] ip route` `<ip-address> <mask> <next-hop> [<next-hop>] [<next-hop>] [<cost>] [<preference>]`

ip-address	The IP address of the network
mask	Mask of the static route
next-hop	The next hop address in the network
cost	The path cost. The default is 1
preference	Preference, either High or Low. Default is Low.

Example:

To define the router 192.168.33.38 as the next hop for the network 192.168.33.0 with mask 255.255.255.0:

```
Router-N(configure)# ip route 192.168.33.0 255.255.255.0
10.10.10.10
```

clear ip route Command

Use the `clear ip route` command to delete all the dynamic routing entries from the Routing Table.

The syntax for this command is:

`clear ip route` `* | <ip-addr> [<ip-mask>]`

ip-addr	IP address
ip-mask	IP mask address

Example:

```
clear ip route *                          clears all the routing table
clear ip route 192.168.49.1 255.255.255.0 clears a range of entries
```

ip routing Command

Use the `ip routing` command to enable IP routing. The `no` form of this command disables the IP routing process in the device. By default, IP routing is enabled.

The syntax for this command is:

`[no] ip routing`

ip max-route-entries Command

This command exists for compatibility with P550. There is no limitation on the size of the routing table, except for the amount of available memory.

The syntax for this command is:

`[no] ip max-route-entries <value>`

value	number of entries

arp Command

Use the `arp` command to add a permanent entry to the Address Resolution Protocol (ARP) cache. The `no` form of this command removes an entry, either a static entry or a dynamically learned entry.

The syntax for this command is:

`[no] arp` `<ip-address> <mac-address>`

ip-address	IP address, in dotted decimal format, of the station
mac-address	MAC address of the local data link

Example:

To add a permanent entry for station 192.168.7.8 to the ARP cache:

`Router(configure)#` **`arp 192.168.7.8 00:40:0d:8c:2a:01`**

To remove an entry to the ARP cache for the station 192.168.13.76:

`Router(configure)#` **`no arp 192.168.13.76`**

arp timeout Command

Use the `arp timeout` command to configure the amount of time that an entry remains in the ARP cache. To restore the default value, 14400, use the `no` form of this command.

The syntax for this command is:

`arp timeout` `<seconds>`

The syntax for the `no form` of this command is:

`no arp timeout`

seconds	The amount of time, in seconds, that an entry remains in the arp cache.

Example:

To set the arp timeout to one hour:

```
Router-N(configure)# arp timeout 3600
```

To restore the default arp timeout:

```
Router-N(configure)# no arp timeout
```

clear arp-cache Command

Use the `clear arp-cache` command to delete all dynamic entries from the ARP cache and the IP route cache.

The syntax for this command is:

```
clear arp cache[<vlan>|<ip addr>[<mask>]]
```

vlan	VLAN string (up to 16 characters
ip addr	IP address
mask	IP mask

```
Example:
clear arp-cache                    flush all arp entries
clear arp-cache marketing_vlan     flush ARP entries for a VLAN
clear arp-cache 192.168.0.0 255.255.0.0  flush range of ARP entries
                                belonging to one subnet
```

ip max-arp-entries Command

Use the `ip max-arp-entries` command to specify the maximum number of ARP cache entries allowed in the ARP cache. The `no` form of this command restores to the default value of 4096. This command takes effect only after start-up.

The syntax for this command is:

`[no] ip max-arp-entries` `<value>`

value	The space available for the IP address table. When you decrease the number of entries, it may cause the table to be relearned more frequently. If you do not enter a value, then the current ARP Cache size is shown.

Example:

To set the maximum number of ARP cache entries to 8000:

```
Router-N(configure)# ip max-arp-entries 8000
```

To restore the maximum number of ARP cache entries to its default:

```
Router-N(configure)# no ip max-arp-entries
```

ip icmp-errors Command

Use the `ip icmp-errors` command to set ICMP error messages ON. The `no` form of this command to set ICMP error messages OFF.

The syntax for this command is:

`[no] ip icmp-errors`

ip netmask-format Command

Use the `ip netmask-format` command to specify the format of netmasks in the **show** command output. The `no` form of this command restores to the default, which is a dotted decimal format.

The syntax for this command is:

`[no] ip netmask-format` `<mask-format>`

The possible mask formats are:

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example 17
decimal	The network masks are in dotted decimal notation. For example, 255.255.255.0.
hexadecimal	The network masks are in hexadecimal format as indicated by the leading 0X. For example, 0XFFFFFF00.

Example:

To display netmasks in bitcount format:

```
Router-N(configure)# ip netmask-format bitcount
```

Interface Mode

ip address Command

Use the `ip address` command to assign an IP address and mask to an interface.

The syntax for this command is:

`ip address` `<ip-address> <mask> [<admin-state>]`

ip address	The IP address assigned to the interface.
mask	Mask for the associated IP subnet
admin-state	The administration status – either Up or Down

Example:

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the interface "marketing":

```
Router-N(config-if:marketing)# ip address 192.168.22.33
255.255.255.0
```

ip vlan/ip vlan name Commands

Use these commands to specify the VLAN on which an IP interface resides. You can specify either the VLAN ID using the `ip vlan` command or the VLAN name using the `ip vlan name` command. The `no` form of the command restores the IP interface to the default VLAN.

The syntax for this command is:

`[no] ip vlan <vlan-id>`

or

`ip vlan name` `<vlan-Name>`

Example:

To specify VLAN developmental as the VLAN used by interface "products":

```
Router-N(config-if:marketing)# ip vlan name development
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

ip admin-state Command

Use the `ip admin-state` command to set the administrative state of an IP interface. The default state is **up**.

The syntax for this command is:

`ip admin-state` <up/down>

up / down	Administrative state of the interface. The choices are **up** (active) or **down** (inactive).

ip netbios-rebroadcast Command

Use the `ip netbios-rebroadcast` command to set NETBIOS rebroadcasts mode on an interface. The `no` form of this command disables NETBIOS rebroadcasts on an interface.

The syntax for this command is:

`[no] ip netbios-rebroadcast` <mode>

The possible values of `mode` are:

both	Netbios packets received on the interface rebrodcasted to other interfaces and netbios packets received on other interfaces are rebroadcasted into this interface.
disable	Netbios packets are not rebroadcasted into or out of this interface.

Example:

To enable rebroadcasting of netbios packets received by and sent from the interface “marketing”:

```
Router-N(config-if:marketing)# ip netbios-rebroadcast both
```

ip directed-broadcast Command

Use the `ip directed-broadcast` command to enable net-directed broadcast forwarding. The `no` form of this command disables net-directed broadcasts on an interface.

The syntax for this command is:

`[no] ip directed-broadcast`

ip proxy-arp Command

Use the `ip proxy-arp` command to enable proxy ARP on an interface. The `no` form of this command disables proxy ARP on an interface.

The syntax for this command is:

`[no] ip proxy-arp`

Example:

To disable proxy ARP on interface marketing:

```
Router-N(config-if:marketing)# no ip proxy-arp
```

ip routing-mode Command

Use the `ip routing-mode` command to set the IP routing mode of the interface. In RT-MGMT mode, the interface functions as a routing interface. In RT_PRIMARY_MGMT mode, the interface function as both a routing interface and the primary management interface. The IP address used in Avaya Multi-Service Network Manager is the primary management interface IP address. Only one interface can be in RT_PRIMARY_MGMT mode. If no interface is configured to RT_PRIMARY_MGMT, the IP address used in Avaya Multi-Service Network Manager is selected randomly.

The syntax for this command is:

`ip routing-mode` `<mode>`

mode	RT_MGMT or RT_PRIMARY_MGMT mode

Example:

```
Router-N>ip routing-mode RT_PRIMARY_MGMT
```

ip redirect Command

Use the `ip redirect` command to enable the sending of redirect messages on the interface. The `no` form of this command disables the redirect messages. By default, sending of redirect messages on the interface is enabled.

The syntax for this command is:

`[no] ip redirect`

Example:

```
Router-N>ip redirect
```

ip broadcast-address Command

Use the `ip broadcast-address` command to update the interface broadcast address. The Broadcast address must be filled in with 0s or 1s.

The syntax for this command is:

`ip broadcast-address` `<bc addr>`

`bc addr`	The broadcast IP address

Example:

```
ip broadcast-address 192.168.255.255
```

enable vlan commands Command

Use the `enable vlan` command before configuring VLAN-oriented parameters, when there is more than one interface on the same VLAN.

The syntax for this command is:

`enable vlan commands`

RIP Commands

Table 6.3 RIP Commands

Configure Mode

router rip Command

Use the `router rip` command to configure the Routing Information Protocol (RIP). The `no` form of this command disables RIP. The default state is **disabled**.

The syntax for this command is:

`[no] router rip`

Example:

To enable the RIP protocol:

```
Router-N(configure)# router rip
```

Router-RIP Mode

redistribute Command

Use the `redistribute` command to redistribute routing information from other protocols into RIP. The `no` form of this command disables redistribution by RIP. The default is **disabled**.

The syntax for this command is:

`[no] redistribute` `<protocol>`

protocol	Either Static or OSPF

Example:

```
Router-N(configure router:rip)# redistribute ospf
```

network Command

Use the `network` command to specify a list of networks on which the RIP is running. The `no` form of this command removes an entry.

The syntax for this command is:

`[no] network` `<ip-address> [<wildcard-mask>]`

ip addr	The IP address of the network of directly connected networks
wildcard-mask	Wildcard mask address. Exists for compatibility with P550.

Example:

To specify that RIP will be used on all interfaces connected to the network 192.168.37.0:

```
Router-N(configure router:rip)# network 192.168.37.0
```

Interface Mode

ip rip rip-version Command

Use the `ip rip rip-version` command to specify the RIP version running on the interface basis.

The syntax for this command is:

`ip rip rip-version` `[1][2]`

The possible versions of the RIP packets received and sent on an interface are:

[1]	RIP Version 1 packets
[2]	RIP Version 2 packets.

Example:

To specify that RIP version 2 should be running on the basis of the interface "marketing":

```
Router-N(config-if:marketing)# ip rip rip version 2
```

default-metric Command

Use the `default-metric` command to set the interface RIP route metric. The `no` form of this command restores the default. The default metric is **1**.

The syntax for this command is:

`[no] default-metric` `<number>`

number	The interface RIP route metric value. The range is 0 to 15.

Example:

To set the default RIP metric value. The range is 0 to 15:

```
Router(config-if:marketing)# default-metric 10
```

ip rip send-receive Command

Use the `ip rip send-receive` command to set the RIP Send and Receive mode on an interface. The default state is **talk-listen**.

The syntax for this command is:

`ip rip send-receive` `<mode>[<default route metric>]`

mode	`talk-listen` - Set RIP to receive and transmit updates on the interface. `talkdefault-listen` - Set RIP to receive updates on the interface and send only a default route.
default route metric	Integer value

Example:

To set the RIP Send and Receive mode on the interface “marketing” to be listen-only:

```
Router-N(config-if:marketing)# ip rip send-receive talk listen
```

ip rip default-route-mode Command

Use the `ip rip default-route-mode` command to enable learning of the default route received by the RIP protocol. The default state is talk-listen.

The syntax for this command is:

`ip rip default-route-mode` `<mode>`

The possible default route modes on an interface are:

talk-listen	Set RIP to send and receive default route updates on the interface.
talk-only	Set RIP to send but not receive default route updates on the interface.

ip rip poison-reverse Command

Use the `ip rip poison-reverse` command to enable split-horizon with poison-reverse on an interface. The `no` form of this command disables the poison-reverse mechanism.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Poison reverse updates explicitly indicate that a network or subnet is unreachable rather than implying they are not reachable. Poison reverse updates are sent to defeat large routing loops.

The syntax for this command is:

`[no] ip rip poison-reverse`

ip rip split-horizon Command

Use the `ip rip split-horizon` command to enable split-horizon mechanism. The `no` form of this command disables the split-horizon. By default split-horizon is enabled.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

The syntax for this command is:

`[no] ip rip split-horizon`

Example:

```
Router-N(config-if:marketing)# no ip rip split-horizon
```

ip rip authentication mode Command

Use the `ip rip authentication mode` command to specify the type of authentication used in RIP Version 2 packets. The `no` form of this command restores the default value of none.

The syntax for this command is: **`[no] ip rip authentication mode`** `[simple|none]`

simple | none	The authentication type used in RIP Version 2 packets: • simple - clear text authentication. • none - no authentication.

Example:

To specify simple authentication to be used in RIP Version 2 packets on the interface “marketing”.

```
Router(config-if:marketing)# ip rip authentication mode simple
```

ip rip authentication key Command

Use the `ip rip authentication key` command to set the authentication string used on the interface. The `no` form of this command clears the password.

The syntax for this command is:

`[no] ip rip authentication key` `<password>`

`password`	The authentication string for the interface. Up to 16 characters are allowed.

Example:

To set the authentication string used on the interface “marketing” to be “hush-hush”.

```
Router-N(config-if:marketing)# ip rip authentication key hush-hush
```

OSPF Commands

Table 6.4 OSPF Commands

User Mode

show ip ospf Command

Use the `show ip ospf` command to display general information about OSPF routing.

The syntax for this command is:

`show ip ospf`

show ip ospf interface Command

Use the `show ip ospf interface` command to display the OSPF-related interface information.

The syntax for this command is:

`show ip ospf interface` `[<interface-name>]`

interface-name	The OSPF interface name.

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

show ip ospf neighbor Command

Use the `show ip ospf neighbor` command to display OSPF-neighbor information on a per-interface basis.

The syntax for this command is: **`show ip ospf neighbor`** `[<interface-name>] [<neighbor-id>]`

interface-name	The OSPF interface name.
neighbor-id	Neighbor ID.

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

show ip ospf database Command

Use the `show ip ospf database` command to display lists of information related to the OSPF database for a specific router.

The syntax for this command is:

`show ip ospf database`
`[{asbr-summary|router|network|network-summary|external}]`

asbr-summary	Displays information only about the autonomous system boundary router summary LSAs. Optional.
external	Displays information only about the external LSAa. Optional.
network	Displays information only about the network LSAa. Optional.
network-summary	Displays information only about the network LSAa summary. Optional
router	Displays information only about the router LSAs. Optional.

Configure Mode

router ospf Command

Use the `router ospf` command to enable OSPF protocol on the system. The `no` form of this command disables it globally. The default is **disabled**.

The syntax for this command is:

`[no] router ospf`

Router-OSPF Mode

area Command

Use the `area` command to configure the area ID of the router. The `no` form of this command deletes the area ID of the router (sets it to 0) and removes the stub definition. The default area is **0.0.0.0**.

Note: You cannot define a stub area when OSPF is redistributing other protocols or when the Area ID is 0.0.0.0.

The syntax for this command is:

[no] area <area id> [<stub>]

area id	IP address
stub	Stub

Example:

```
Router-N(configure router:ospf)# area 192.168.49.1
Router-N(configure router:ospf)# area 192.168.49.1 stub
```

network Command

Use the `network` command to enable OSPF in this network. The `no` form of this command disables the OSPF in this network. The default is **disabled**.

The syntax for this command is:

network <net addr> [<wildcard-mask> [area <area id>]]

net addr	IP address
wildcard-mask	Wildcard mask address
area id	Area ID. This parameter exists for compatibility with P550.

Example:

```
Router-N(configure router:ospf)# network 192.168.0.0
Router-N(configure router:ospf)# network 192.168.0.0
0.0.255.255 area 0.0.0.0
```

ip ospf router-id Command

Use the `ip ospf router-id` command to configure router identity. The `no` form of this command returns the router identity to its default (lowest IP interface that exists).

The syntax for this command is:

`[no] ip ospf router-id` `<router id>`

router id	IP address

Example:

```
Router-N# ip ospf router-id 192.168.49.1
```

redistribute Command

Use the `redistribute` command to redistribute routing information from other protocols into OSPF. The `no` form of this command disables redistribution by OSPF.

The syntax for this command is:

`[no] redistribute` `<protocol>`

protocol	[static | ospf]

Example:

```
Router-N(configure router:ospf)# redistribute static
```

timers spf Command

Use the `timers spf` command to configure the delay between runs of OSPF's SPF calculation. Use the `no` form of this command to restore the default (3 seconds).

The syntax for this command is:

`[no] timers spf` `<spf-holdtime>`

spf-holdtime	The time in seconds of the delay between runs of OSPF's SPF calculation.

Example:

```
Router-N(configure router:ospf)# timers spf 5
```

Interface Mode

ip ospf cost Command

Use the `ip ospf cost` command to configure interface metric. The `no` form of this command sets the cost to its default. The default is **1**.

The syntax for this command is:

`[no] ip ospf cost` `<cost>`

cost	integer

Example:

```
ip ospf cost 10
```

ip ospf hello-interval Command

Use the `ip ospf hello-interval` command to specify the time interval between hello's the router sends. The `no` form of this command sets the hello-interval to its default. The default is **10**.

The syntax for this command is:

`[no] ip ospf hello-interval` `<seconds>`

seconds	integer

Example:

```
ip ospf hello-interval 5
```

ip ospf dead-interval Command

Use the `ip ospf dead-interval` command to configure the interval before declaring the neighbor as dead. The `no` form of this command sets the dead-interval to its default. The default is **40**.

The syntax for this command is:

`[no] ip ospf dead-interval` `<seconds>`

seconds	integer

Example:

```
ip ospf dead-interval 15
```

ip ospf priority Command

Use the `ip ospf priority` command to configure interface priority used in DR election. The `no` form of this command sets the OSPF priority to its default. The default is **1**.

The syntax for this command is:

`[no] ip ospf priority` `<priority>`

priority	integer

Example:

```
priority 17
```

ip ospf authentication-key Command

Use the `ip ospf authentication-key` command to configure the interface authentication password. The `no` form of this command removes the OSPF password.

The syntax for this command is:

`[no] ip ospf authentication-key` `<key>`

key	string (up to 8 characters)

Example:

```
ip ospf authentication-key my_pass
```

VRRP Commands

Table 6.5 VRRP Commands

User Mode

show ip vrrp Command

Use the `show ip vrrp` command to display VRRP information.

The syntax for this command is:

`show ip vrrp` `[<vlan> [router-id <vr-id>]][detail]`

vlan	Filter by VLAN.
router-id	Filter by virtual router ID.
vr-id	The virtual router ID.
detail	Provide detailed information.

Output Example:

```
Router-1> show ip vrrp
VRRP is globally enabled
VLAN   VRID    IP Address      Pri    Timer    State       Since
------  ------   ---------------   ----   -------  ---------    -----------
 1       1      192.168.66.23   255    1      MASTER    00:00:00
 1       2      192.168.66.24   100    1      BACKUP    00:00:00
```

show ip vrrp detail Command

Use the `show ip vrrp detail` command to display full VRRP-related information

The syntax for this command is:

`show ip vrrp detail`

detail	Show full detail information

Output Example:

```
Router-1> show ip vrrp detail
VRRP is globally enabled
Virtual Router on VLAN:                                    1
    Router-id:                                             1
    State:                                            MASTER
    Priority:                                            255
    Advertisement Interval:                                1
    Last State Change:                              00:00:00
    Override Address Ownership Rule: No
    Authentication Type:                                None
    Authentication Key:       ""
    Master IP Address                          192.168.66.23
    Has 1 IP addresses
    IP addresses:
      192.168.66.23
    Primary IP Address:                        192.168.66.23
    Primary IP Address was chosen by default
    Preemption Mode:          enabled
    # of times Master:                                     2
    # of received Advertisements:                         0
    # of transmitted Advertisements:                      20
    # of received Advertisements with Security Violations: 0
Virtual Router on VLAN:       1
    Router-id:                2
    State:                    BACKUP
    Priority:                 100
    Advertisement Interval:   1
    Last State Change:        00:00:00
    Override Address Ownership Rule: No
    Authentication Type:      None
    Authentication Key:       ""
```

```
Master IP Address         0.0.0.0
Has 1 IP addresses
IP addresses:
  192.168.66.24
Primary IP Address:       192.168.66.23
Primary IP Address was chosen by default
Preemption Mode:          enabled
# of times Master:                                    1
# of received Advertisements:                        0
# of transmitted Advertisements:                     13
# of received Advertisements with Security Violations: 0
```

Configure Mode

router vrrp Command

Use the `router vrrp` command to enable VRRP routing globally. Use the `no` form of this command to disable VRRP routing.

Note: You cannot activate both VRRP and SRRP protocols at the same time.

The syntax for this command is:

`[no] router vrrp`

Interface Mode

ip vrrp Command

Use the `ip vrrp` command to create a virtual router on the interface. Use the `no` form of this command to delete a virtual router.

The syntax for this command is:

`[no] ip vrrp` `<vr-id>`

vr-id	Virtual Router ID (1-255)

Example:

```
Router-N(config-if:marketing)# ip vrrp 1
```

ip vrrp address Command

Use the `ip vrrp address` command to assign an IP address to the virtual router. Use the `no` form of this command to remove an IP address from a virtual router.

The syntax for this command is:

`[no] ip vrrp` `<vr-id>` **`address`** `<ip-address>`

vr-id	Virtual Router ID (1-255)
ip-address	The IP address to be assigned to the virtual router.

Example:

To assign address 10.0.1.2 to virtual router 1:

```
Router(config-if:marketing)# ip vrrp 1 address 10.0.1.2
```

ip vrrp timer Command

Use the `ip vrrp timer` command to set the virtual router advertisement timer value (in seconds) for the virtual router ID. Use the `no` form of this command to restore the default value.

The syntax for this command is: **`[no] ip vrrp`** `<vr-id>` **`timer`** `<value>`

vr-id	Virtual Router ID (1-255)
value	The advertisement transmit time (seconds).

Example:

To set the virtual router advertisement timer value for virtual router 3 to 2:

```
Router-N(config-if:marketing)# ip vrrp 3 timer 2
```

ip vrrp priority Command

Use the `ip vrrp priority` command to set the virtual router priority value used when selecting a master router. Use the `no` form of this command to restore the default value.

The syntax for this command is:

`[no] ip vrrp` `<vr-id>` **`priority`** `<pri-value>`

vr-id	Virtual Router ID (1-255)
pri-value	The priority value. The range is 1-254.

Example:

To set the priority value for virtual router 1 to 10:

```
Router-N(config-if:marketing)# ip vrrp 1 priority 10
```

Ip vrrp auth-key Command

Use the `ip vrrp auth-key` command to set the virtual router simple password authentication for the virtual router ID. Use the no form of this command to disable simple password authentication for the virtual router instance.

The syntax for this command is:

[no] ip vrrp <vr-id> **auth-key** <key-string>

vr-id	Virtual Router ID (1-255)
key-string	Simple password string.

Ip vrrp preempt Command

Use the `ip vrrp preempt` command to configure the router to preempt a lower priority master for the virtual router ID. Use the no form of this command to disable preemption for the virtual router instance. By default, preemption is enabled.

The syntax for this command is:

[no] ip vrrp <vr-id> **preempt**

vr-id	Virtual Router ID (1-255)

Example:

```
Router-N(config-if:marketing)# ip vrrp 1 preempt
```

Ip vrrp primary Command

Use the `ip vrrp primary` command to set the primary address that shall be used as the source address of VRRP packets for the virtual router ID. Use the no form of this command to return to the default primary address for the virtual router instance. By default, the primary address is selected automatically by the device.

The syntax for this command is:

[no] ip vrrp <vr-id> **primary** <ip-address>

vr-id	Virtual Router ID (1-255)
ip-address	Primary IP address of the virtual router. This address should be one of the router addresses on the VLAN.

Example:

```
ip vrrp 1 primary 192.168.66.23
```

Ip vrrp override addr owner Command

Use the `ip vrrp override addr owner` command to accept packets addressed to the IP address(es) associated with the virtual router, such as ICMP, SNMP, and TELNET (if it is not the IP address owner). Use the no form of this command to discard these packets.

The syntax for this command is:

[no] ip vrrp <vr-id> **override addr owner**

vr-id	Virtual Router ID (1-255)

Example:

```
Router-N(config-if:marketing)# ip vrrp 1 override addr owner
```

SRRP Commands

Table 6.6 SRRP Commands

Command	Page
show ip srrp	177
router srrp	178
ip srrp backup	179
poll-interval	178
timeout	178

User Mode

show ip srrp Command

Use the `show ip srrp` to display the SRRP configuration and status.

The syntax for this command is:

`show ip srrp`

Output Example::

```
Router> show ip srrp
Admin status   Oper State   Poll interval   Timeout
============   ==========   =============   =======
DISABLE        INACTIVE            1           12

Showing 3 rows
Intf IP addr      Main router addr
===============   ================
192.168.1.1         192.168.1.2
192.168.2.1         192.168.2.2
192.168.3.1         192.168.3.2
```

Configure Mode

router srrp Command

Use the `router srrp` command to configure SRRP options, activate SRRP and enter the SRRP configuration mode. The `no` form of this command disables it globally. The default is **disabled**.

Note: You cannot activate both VRRP and SRRP protocols at the same time.

The syntax for this command is:

`[no] router srrp`

Router-SRRP Mode

poll-interval Command

Use the `poll-interval` command to configure the polling interval in seconds used by SRRP. Use the `no` form of this command to return to the default polling interval of 1 second.

The syntax for this command is:

`[no] poll-interval` `<poll interval>`

poll interval	An integer (in seconds)

Example:

```
Router-N(configure router:srrp)# poll-interval 4
```

timeout Command

Use the `timeout` command to configure the timeout (in seconds) after which SRRP declares the main router dead if it does not reply to polling.

Use the `no` form of this command to return to default timeout interval of 12 seconds.

The syntax for this command is:

`[no] timeout <timeout>`

`timeout`	An integer (in seconds)

Example:

```
Router-N(configure router:srrp)# timeout 6
```

Interface Mode

ip srrp backup Command

Use the `ip srrp backup` to backup an additional interface of the main router using the SRRP application. If the main router fails, the P332-ML takes over its activities on all configured interfaces.

The syntax for this command is:

`ip srrp backup` `<main router addr>`

main router addr	IP address of the interface

Example:

```
Router-N(config-if:marketing)# ip srrp backup 192.168.50.11
```

BOOTP-DHCP Commands

Table 6.7 BOOTP-DHCP Commands

Configure Mode

ip bootp-dhcp relay Command

Use the `ip bootp-dhcp relay` command to enable relaying of bootp and dhcp requests to the bootp / dhcp server. The no form of this command disables bootp / dhcp relay. The default state is: **`disabled`**.

The syntax for this command is:

`[no] ip bootp-dhcp relay`

Example:

To enable relaying of BOOTP and DHCP requests:

```
Router-N(configure)# ip bootp-dhcp relay
```

To disable relaying of bootp and dhcp requests:

```
Router-N(configure)# no ip bootp-dhcp relay
```

Interface Mode

ip bootp-dhcp server Command

Use the `ip bootp-dhcp server` command to add a bootp / dhcp server to handle bootp / dhcp requests received by this interface. The no form of this command removes the server. A maximum of two servers can be added to a single interface.

The syntax for this command is:

`ip bootp-dhcp server` `<ip-address>`

ip-address	The IP address of the server.

Example:

To add station 192.168.37.46 as a bootp / dhcp server to handle bootp / dhcp requests arriving at the interface “marketing”:

```
Router-N(config-if:marketing)# ip bootp-dhcp server
192.168.37.46
```

ip bootp-dhcp network Command

Use the `ip bootp-dhcp network` command to select the network from which the bootp / dhcp server shall allocate an address. This command is required only when there are multiple interfaces over the VLAN. The `no` form of this command restores to the default.

The syntax for this command is:

`[no] ip bootp-dhcp network` `<ip-address>`

`ip-address`	The IP address of the network.

Example:

To select the network 192.168.169.0 as the network from which an address shall be allocated for bootp / dhcp requests:

```
Router-N(config-if:marketing)# ip bootp-dhcp network
192.168.169.0
```

Policy Commands

Table 6.8 Policy Commands

User Mode

show access-group command

Use the `show` access-group to see information about the configured active access list.

The syntax for this command is:

`Show access-group`

```
Example:
Router-N> show access-group
access-group 100
```

show ip access lists Command

Use the `show ip access-lists` command to see all the current policy lists.

The syntax for this command is:

`Show ip access-lists[<policy-list-number>]`

policy-list-number	The policy list number (integer from 100 to 199)

Example:

```
Router-N> show ip access-lists

 ip access-list 100 10 deny-and-notify tcp
   192.168.55.0      0.0.0.255       range  5000  6000
   any range  7000  8000
 ip access-list 100 30 deny udp
   any
   any
   optional
 ip access-list 100 35 deny ip
   any
   any
 ip access-list 100 55 fwd7 tcp
   host 192.168.3.4         eq    33333
   host 10.6.7.8
 default action for list 100 is permit
```

show dscp Command

Use the `show dscp` command to see the DSCP table.

The syntax for this command is:

`Show dscp[<dscp>]`

dscp	dscp entry

Example:

```
Router-N> show dscp

 set qos trust trust-cos-dscp
 DSCP  Action  Agg Idx                    Name
 ----  ------  -------  ---------------------------------------
    0  fwd0          0  DSCP #0
    1  fwd0          0  DSCP #1
    2  fwd0          0  DSCP #2
    3  fwd0          0  DSCP #3
    4  fwd0          0  DSCP #4
    5  fwd0          0  DSCP #5
    6  fwd0          0  DSCP #6
    7  fwd0          0  DSCP #7
    8  fwd1          1  DSCP #8
    9  fwd1          1  DSCP #9
   10  fwd1          1  DSCP #10
   ...
   62  fwd7          7  DSCP #62
   63  fwd7          7  DSCP #63
```

Configure Mode

ip access-group Command

Use the `ip access-group` command to activate a specific policy list. To deactivate the policy list, use the no version of this command.

The syntax for this command is:

`[no] ip access-group` `<policy-list-number>[<default-action>]`

<priority-list-number>	integer (100..199)
<default-action>	default-action-deny | default-action-permit

Example:

```
Router-N>ip access-group 101
```

ip access-list Command

Use the `ip access-list` command to create a specific policy rule. This command defines a policy rule. The access list contains several of these rules. Each rule pertains to the source IP address, the destination IP address, the protocol, the protocol ports (if relevant), and to the ACK bit (if relevant).

The syntax for this command is:

```
[no] ip access-list <access-list-number> <access-list-index>
                    <command> <protocol> {<source-ip>
                    <source-wildcard> | any |host
                    <source-ip>}[<operator> <port> [<port]]
                    {<destination-ip> <destination-
                      wildcard>|any |host
                    <destination-ip>}[<operator> <port>
                   [<port>]][established] [precedence]
```

<access-list-number>	integer (100..149)
<access-list-index>	integer (1...9999)
<command>	permit | deny | deny-and-notify | fwd0-7
<protocol>	ip | tcp | udp | integer (1..255)
<source-ip>	ip network
<source-wildcard>	ip network wildcard
<operator>	eq | lt | gt | range
<port>	integer (1..65535)
<destination-ip>	ip network
<destination-wildcard>	ip network wildcard
<precedence>	mandatory | optional]

Example:

```
Router-N>ip access-list 101 23 deny ip any
         1.2.0.0 0.0.255.255
```

To delete a specific rule, use the `no` form of this command.

ip access-default-action Command

Use the `ip access-default-action` command to set the default action for a specific policy list.

The syntax for this command is:

`ip access-default-action` `<policy-list-number> <default-action>`

<policy-list-number>	integer (100..199)
<default-action>	default-action-deny | default-action-permit

Example:

```
Router-N>ip access-default-action 101 default-action-deny
```

ip access-list-name Command

Use the `ip access-list-name` command to set a name for a policy list.

The syntax for this command is:

`ip access-list-name` `<policy-list-number> <name>`

<policy-list-number>	integer (100..199)
<name>	list name

Example:

```
Router-N>ip access-list-name 101 morning
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

ip access-list-owner Command

Use the `ip access-list-owner` command to set the owner for a specific policy list.

The syntax for this command is:

`ip access-list-owner` `<policy-list-number> <owner>`

<policy-list-number>	integer (100..199)
<owner>	list owner

Example:

```
Router-N>ip access-list-owner 101 admin
```

ip access-list-cookie Command

Use the `ip access-list-cookie` command to set the list cookie for a specific policy list.

The syntax for this command is:

`ip access-list-cookie` `<policy-list-number> <cookie>`

<policy-list-number>	integer (100..199)
<cookie>	integer

Example:

```
Router-N>ip access-list-cookie 101 12345
```

ip access-list-copy Command

Use the `ip access-list-copy` command to copy a configured source policy list to a destination policy list.

The syntax for this command is:

`ip access-list-copy` `<source-list> <destination-list>`

<source-list>	integer (100..199)
<destination-list>	integer (100..199)

Example:

```
Router-N>ip access-list-copy 100 101
```

ip simulate Command

Use the `ip simulate` command to check the policy for a simulated packet. The command contains the addressed list number, and the packet parameters.

The syntax for this command is:

`ip simulate` `<access-list-number> [<priority>] [<dscp-value>]<source> <destination> [<protocol> [<source port> <destination port> [<established>]]]`

access-list-number	integer (100..199)
priority	fwd0 | fwd1 | .. | fwd7
dspc value	dscp0 | dscp1 | .. | dscp63
source	source ip address
destination	destination ip address
protocol	ip | tcp | udp | integer (1..255)
source port	integer (1..65535)
destination port	integer (1..65535)
established	value of TCP established bit

Example:

```
Router-N>ip simulate 100 192.67.85.12 193.76.54.25
```

validate-group Command

Use the `validate-group` command to verify that all the rules in a priority list are valid.

If there is a configuration problem with a specific rule, or with a number of rules, detailed error messages will be given.

The syntax for this command is:

`validate-group` `<policy-list-number>[quiet]`

`quiet - does not display error messages`

```
Example:
Router-N(configure)# validate-group 101
```

set qos policy-source Command

Use the `set qos policy-source` command to set the policy source. The default policy source is policy-server.

Note: Before configuring the IP access list, you must change the policy source mode to local.

The syntax for this command is:

```
set qos policy-source <source>
<source>  - local | policy-server
```

Example:

```
Router-N(configure)# set qos policy-source local
```

set qos dscp-cos-map Command

Use the `set qos dscp-cos-map` command to configure the DSCP table.

The syntax for this command is:

```
set qos dscp-cos-map <dscp1>[-<dscp2>] <operation>
[<precedence>]
<dscp1>       - dscp range min (0-63)
<dscp2>       - dscp range max (0-63)
<operation>   - fwd0-7 | no-change
<precedence>  - mandatory | optional
```

Example:

```
Router-N(configure)#set qos dscp-cos-map 9-16 fwd3
```

set qos dscp-name Command

Use the `set qos dscp-name` command to configure the DSCP entry name.

The syntax for this command is:

```
set qos dscp-name <dscp> <name>
<dscp>       - DSCP entry (0-63)
<name>       - entry name
```

Example:

```
Router-N(configure)# set qos dscp-name 10 "special"
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

set qos trust Command

Use the set qos trust command to configure which of the incoming packet's priority parameters should be considered when determining the new assigned priority. You can configure the P332G-ML to trust either the cos (the 802.1p priority), the dscp (the DSCP value), or neither. The default value is trust-cos. P332G-ML does not support trust-cos-dscp.

The syntax for this command is:

```
set qos trust {untrusted  | trust-cos | trust-dscp | trust-
cos-dscp}
```

Example:

```
Router-N(configure)# set qos trust-cos
```

VLAN Commands

Table 6.9 VLAN Commands

User Mode

show vlan Command

Use the `show vlan` command to display router Layer 2 interfaces.

The syntax for this command is:

`show vlan` `[details]`

Configure Mode

set vlan Command

Use the `set vlan` command to create router Layer 2 interface.

The syntax for this command is:

`set vlan` `<vlan-id>` **`name`** `<vlan-name>`

vlan-id	Interface Index
vlan-name	Interface name (used in layer 3 protocols)

```
Example:
Router-N(configure)# set vlan 2 name vlan2
```

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

clear vlan Command

Use the `clear vlan` command to Delete Router layer 2 interface.

The syntax for this command is:

`clear vlan` `[<vlan-id>] | [name <vlan-name>]`

vlan-id	Interface Index
vlan-name	Interface name (used in layer 3 protocols)

Note: If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

Tech Command

Use the `tech` command to enter tech mode. This command is reserved for service personnel use only.

P330 Embedded Web Manager

The P330 Embedded Web Manager provides the following:

- Device Configuration - Viewing and modifying the different device configurations.
- Virtual LANs - Viewing and editing Virtual LAN information.
- Link Aggregation Groups (LAGs) - Viewing and editing LAG information.
- Software Redundancy - Setting software redundancy for ports in a P330 Switch.
- Port Mirroring - Setting up port mirroring for ports in a P330 Switch.
- Trap Managers Configuration - Viewing and modifying the Trap Managers Table.
- Switch Connected Addresses - View devices connected to selected ports.
- Routing Manager - Viewing configurations of IP Routing protocols and general information.

System Requirements

Minimum hardware and Operating System requirements are:

- One of the following operating systems:
  - Windows® 95
  - Windows 98 SP1
  - Windows 98 OSR (Second Edition)
  - Windows ME
  - Windows NT® Workstation or Server
  - Windows 2000 Professional or Server
- Pentium® II 400 Mhz-based computer with 256 Mb of RAM (512 Mb recommended)
- Minimum screen resolution of 1024 x 768 pixels
- Sun Microsystems Java™ plug-in version 1.2.2 (supplied)

- Microsoft® Internet Explorer® **or** Netscape Navigator/Communicator® (see table)

	Windows 95 or NT	Windows 98, ME or 2000
Internet Explorer	5.0 or higher	5.01 or higher
Netscape Navigator/ Communicator	4.7	4.73

Note for users of Netscape Navigator: The Java plug-in requires certain services from **Windows 95** which are not present if **Internet Explorer** is not installed. In order to add these services to the operating system, please install Internet Explorer version 3 or higher. You can then use either browser to manage the switch.

Running the Embedded Manager

Note: You should assign an IP address to the switch before beginning this procedure.

1 Open your browser.
2 Enter the URL of the switch in the format **`http://aaa.bbb.ccc.ddd`** where ***`aaa.bbb.ccc.ddd`*** is the IP address of the switch.

Note: The user name is “root”
The default password for read-only access is “root”
The default passwords for read-write access are “enable” or “super”.

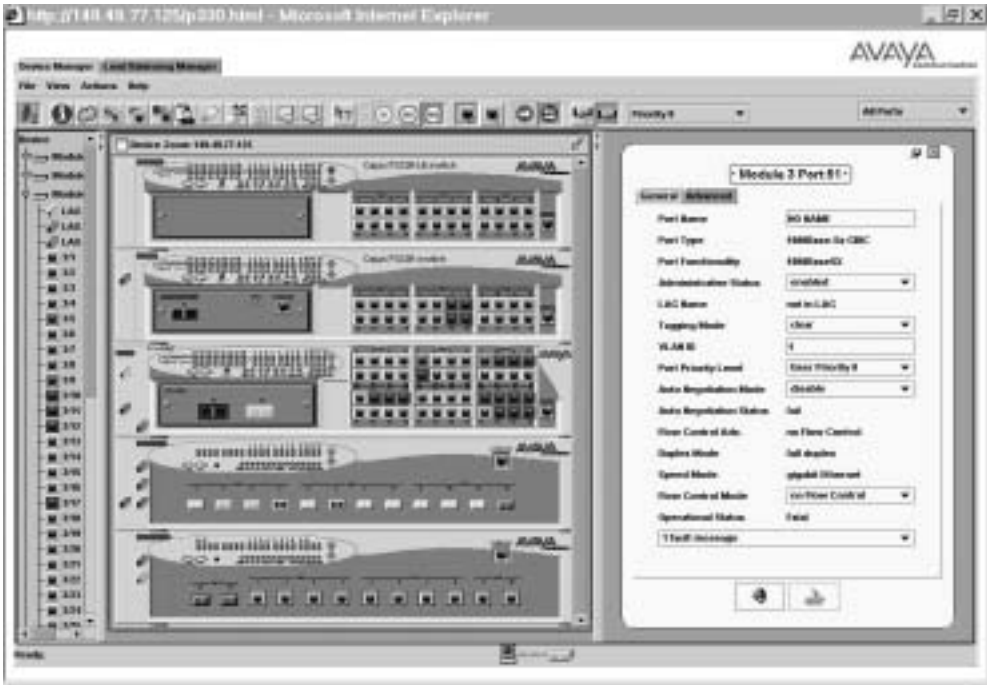
Note: The Web management passwords are the same as those of the CLI. If you change the passwords of the CLI then use those passwords for Web management as well.

3 The welcome page is displayed.

Figure A.1 The Welcome Page

— If you have the Java plug-in installed, the Web-based manager should open in a new window (see Figure A.2)

Figure A.2 Web-based Manager



— If you do **not** have the Java plug-in installed, follow the instructions on the Welcome page that offers a variety of options to install the plug-in.

Installing the Java Plug-in

If the network manager has configured the system, the plug-in should be installed automatically.

If the plug-in is not installed automatically, then you have three options for installing it manually:

1 Installing from the P330 Documentation and Utilities CD

1 Close all unnecessary applications on your PC.
2 Insert the "Avaya P330 Documentation and Utilities" CD into the CD drive.
3 Click **Start** on the task bar.
4 Select Run.
5 Type ***x:*****\emweb-aux-files\plug-in_1_2_2.exe** where ***x:*** is the CD drive letter.
6 Follow the instructions on screen.

2 Install from the Avaya Site

Click on the link in the Welcome page.

3 Install from your Local Web Site

Click on the link in the Welcome page.

Note: This option is only available if the network manager has placed the files on the local Web server.

Installing the On-Line Help and Java Plug-In on your Web Site

Note: This procedure is optional

Copying the help files and Java plug-in to a local Web server allows users to access the on-line help for the Embedded Manager and enables automatic installation of the Java plug-in the first time the users tries to manage the device.

1 Copy the `emweb-aux-files` directory from the "Avaya P330 Documentation and Utilities" CD to your local Web server. Please refer to your Web server documentation for full instructions.

2 Define the URL in the P330 using the following CLI command:
`set web aux-files-url` ***`//IP address/directory name`***
where ***`//IP address/directory name`*** is the location of the directory from the previous step.

Documentation

The Device Manager comes with a detailed User's Guide including a Glossary of Terms and an overview of Data Communications concepts.

Software Download

You can perform software download using the CLI (see "Show tftp download / upload status Command" on page 71) or Cajun UpdateMaster (part of the Avaya Multi-Service Network Manager management suite).

Specifications

P332G-ML Switch

Physical

Height	2U (88 mm, 3.5”)
Width	482.6 mm (19”)
Depth	450 mm(17.7”)
Weight	7.6 kg (16.8 lb)

Power Requirements

	AC	DC
Input voltage	90 to 265 VAC, 50/60 Hz	-36 to -72 VDC
Power dissipation	100 W max	100 W (max.)
Input current	1.5 A@100 VAC 0.75 A@200VAC	4 A (max.)
Inrush current	15 A@100 VAC (max.) 30 A@200VAC (max.)	40 A (max.)

Environmental

Operating Temp.	-5 to 50°C (23-122°F)
Rel. Humidity	5% to 95% non-condensing

Safety — AC

- UL for US approved according to UL195O Std.
- C-UL(UL for Canada) approved according to C22.2 No.950 Std.
- CE for Europe approved according to EN 60950 Std.
- Laser components are Laser Class I approved:
  - — EN-60825/IEC-825 for Europe
  - — FDA CFR 1040 for USA
- Overcurrent Protection: A readily accessible Listed safety-approved protective device with a 16A rating must be incorporated in series with building installation AC power wiring for the equipment under protection.

EMC Emissions

Emissions

Approved according to:

- US - FCC Part 15 sub part B, class A
- Europe - EN55022 class A and EN61000-3-2
- Japan - VCCI-A

Immunity

Approved according to:

- EN 55024 and EN61000-3-3

Interfaces

- P332G-ML: 12 x SFP pluggable Gigabit Ethernet fiber optic connectors.
- RS-232 for terminal setup via RJ-45 connector on front panel.

Standards Compliance

The P332G-ML complies with:

IEEE

- IEEE 802.3x Flow Control
- IEEE 802.1q/p VLAN Tagging and 802.1p compatible
- IEEE 802.1D Spanning Tree protocol
- IEEE 803.3z Gigabit Ethernet ports

IETF

- MIB-II - RFC 1213
- Bridge MIB for Spanning Tree - RFC 1493
- RMON - RFC 1757
- SMON - RFC 2613

Routing

- RIP1
- RIP2
- OSPF
- ARP
- ICMP
- DHCP/BOOTP Relay

Basic MTBF

- P332G-ML: 106,086 hrs minimum.
- P332G-ML and X330STK-ML: 101,936 hrs minimum.

Stacking Sub-module

Table B.1 Stacking Sub-module

Name	Number of Ports
X330STK-ML	2

Basic MTBF

- 2,605,528 hrs minimum

Approved SFF/SFP GBIC Transceivers

The SFF/SFP GBIC (Gigabit Interface Converter) have been tested for use with the Avaya P332G-ML Gigabit Ethernet ports. For a list of approved SFF/SFP GBIC transceivers, see: www.avayanetwork.com/

Note: SFF/SFP GBIC transceivers are hot-swappable.

Safety Information

The SFF/SFP GBIC transceivers are Class 1 Laser products. They comply with EN 60825-1 and Food and Drug Administration (FDA) 21 CFR 1040.10 and 1040.11.

The SFF/SFP GBIC transceivers must be operated under recommended operating conditions.

Laser Classification

Note: Class 1 lasers are inherently safe under reasonably foreseeable conditions of operation.

Caution: The use of optical instruments with this product will increase eye hazard.

Usage Restriction

When a SFF/SFP GBIC transceiver is inserted in the module but is not in use, the Tx and Rx ports should be protected with an optical connector or a dust plug.

Caution: Use only approved SFF/SFP GBIC transceivers. All approved SFF/SFP GBIC transceivers:
1) Are 3.3V. Do **not** insert a 5V SFF/SFP GBIC.
2) Use Serial Identification. Do **not** use a GBIC that utilizes Parallel Identification.

Installation

Installing and Removing a SFF/SFP GBIC Transceiver

Caution: Use only 3.3V Avaya-authorized SFF / SFP GBIC transceivers. Use only SFF / SFP GBIC transceivers that use Serial Identification.

The SFF / SFP GBIC transceiver is fastened using a snap-in clip.

To Install the SFF/SFP GBIC transceiver:

- Insert the transceiver (take care to insert it the right way up) until it clicks in place.

To Remove the SFF/SFP GBIC transceiver:

1 Press the clip on the bottom side of the transceiver.
2 Pull the transceiver out.

Specifications

LX Transceiver

A 9 µm or 10 µm single-mode fiber (SMF) cable may be connected to a 1000Base-LX SFF / SFP GBIC port. The maximum length is 10 km (32,808 ft).

A 50 µm or 62.5 µm multimode (MMF) fiber cable may be connected to a 1000Base-LX SFF / SFP GBIC port. The maximum length is 550 m (1,804 ft.) for 50 µm and 62.5 µm cable.

The LX transceiver has a Wavelength of 1300 nm, Transmission Rate of 1.25 Gbps, Input Voltage of 3.3V, and Maximum Output Wattage of -3 dBm.

SX Transceiver

A 50 µm or 62.5 µm multimode (MMF) fiber cable may be connected to a 1000Base-SX SFF / SFP GBIC port. The maximum length is 500 m (1,640 ft.) for 50 µm and 220 m (722 ft.) for 62.5 µm cable.

The SX transceiver has a Wavelength of 850 nm, Transmission Rate of 1.25 Gbps, Input Voltage of 3.3V, and Maximum Output Wattage of -4 dBm.

Agency Approval

The transceivers comply with:

- EMC Emission: US – FCC Part 15, Subpart B, Class A;
  Europe – EN55022 class A
- Immunity: EN50082-1

Safety: UL for US UL 1950 Std., C-UL (UL for Canada) C22.2 No.950 Std., Food and Drug Administration (FDA) 21 CFR 1040.10 and 1040.11, and CE for Europe EN60950 Std. Complies with EN 60825-1.

Gigabit Fiber Optic Cabling

Table B.2 Gigabit Fiber Optic Cabling

Gigabit Interface	Fiber Type	Diameter (μm)	Modal Bandwidth (MhzKm)	Maximum Distance (m)	Minimum Distance (m)	Wavelength (nm)
1000BASE-SX	MM	62.5	160	220	2	850
1000BASE-SX	MM	62.5	200	275	2	850
1000BASE-SX	MM	50	400	500	2	850
1000BASE-SX	MM	50	500	550	2	850
1000BASE-LX	MM	62.5	500	550	2	1310
1000BASE-LX	MM	50	400	550	2	1310
1000BASE-LX	SM	9	NA	10,000	2	1310

Connector Pin Assignments

Console Pin Assignments

For direct Console communications, connect the Avaya P330 to the Console Terminal using the supplied RJ-45 crossed cable and RJ-45 to DB-9 adapter.

Table B.3 Pinout of the Required Connection for Console Communications

Avaya P330 RJ-45 Pin	Name	Terminal DB-9 Pins	Modem DB-25 Pins
1	For future use	NC	See note
2	TXD (P330 input)	3	3
3	RXD (P330 output)	2	2
4	CD	4	8
5	GND	5	7
6	DTR	1	20
7	RTS	8	4
8	CTS	7	5

Note: Pin 1 of the Modem DB-25 connector is internally connected to Pin 7 GND.

CLI – Layer 2 Command Index

CLI – Layer 3 Command Index

How to Contact Us

To contact Avaya's technical support, please call:

In the United States

Dial 1-800-237-0016, press 0, then press 73300.

In the EMEA (Europe, Middle East and Africa) Region

Country	Local Dial-In Number
Albania	+31 70 414 8001
Austria	+43 1 36 0277 1000
Azerbaijan	+31 70 414 8047
Bahrain	+800 610
Belgium	+32 2 626 8420
Belorussia	+31 70 414 8047
Bosnia Herzegovina	+31 70 414 8042
Bulgaria	+31 70 414 8004
Croatia	+31 70 414 8039
Cyprus	+31 70 414 8005
Czech Rep.	+31 70 414 8006
Denmark	+45 8233 2807
Egypt	+31 70 414 8008
Estonia	+372 6604736
Finland	+358 981 710 081

Country	Local Dial-In Number
France	+33 1 4993 9009
Germany	+49 69 95307 680
Ghana	+31 70 414 8044
Gibraltar	+31 70 414 8013
Greece	+00800 3122 1288
Hungary	+06800 13839
Iceland	+0800 8125
Ireland	+353 160 58 479
Israel	+1 800 93 00 900
Italy	+39 02 7541 9636
Jordan	+31 70 414 8045
Kazakhstan	+31 70 414 8020
Kenya	+31 70 414 8049
Kuwait	+31 70 414 8052
Latvia	+371 721 4368

Country	Local Dial-In Number
Lebanon	+31 70 414 8053
Lithuania	+370 2 756 800
Luxemburg	+352 29 6969 5624
Macedonia	+31 70 414 8041
Malta	+31 70 414 8022
Mauritius	+31 70 414 8054
Morocco	+31 70 414 8055
Netherlands	+31 70 414 8023
Nigeria	+31 70 414 8056
Norway	+47 235 001 00
Oman	+31 70 414 8057
Pakistan	+31 70 414 8058
Poland	+0800 311 1273
Portugal	+351 21 318 0047
Qatar	+31 70 414 8059
Romania	+31 70 414 8027
Russia	+7 095 733 9055
Saudi Arabia	+31 70 414 8022

Country	Local Dial-In Number
Slovakia	+31 70 414 8066
Slovania	+31 70 414 8040
South Africa	+0800 995 059
Spain	+34 91 375 3023
Sweden	+46 851 992 080
Switzerland	+41 22 827 8741
Tanzania	+31 70 414 8060
Tunisia	+31 70 414 8069
Turkey	+800 4491 3919
UAE	+31 70 414 8036
Uganda	+31 70 414 8061
UK	+44 0207 5195000
Ukraine	+31 70 414 8035
Uzbekistan	+31 70 414 8046
Yemen	+31 70 414 8062
Yugoslavia	+31 70 414 8038
Zimbabwe	+31 70 414 8063

Email: csctechnical@avaya.com

In the AP (Asia Pacific) Region

Country	Local Dial-In Number
Australia	+1800 255 233
Hong Kong	+2506 5451
Indonesia	+800 1 255 227
Japan	+0 120 766 227
Korea	+0 80 766 2580

Country	Local Dial-In Number
Malaysia	+1800 880 227
New Zealand	+00 800 9828 9828
Philippines	+1800 1888 7798
Singapore	+1800 872 8717
Taiwan	+0 80 025 227

Email: sgcoe@avaya.com

In the CALA (Caribbean and Latin America) Region

Email: caladatasupp@avaya.com

Hot Line:+1 720 4449 998

Fax:+1 720 444 9103

For updated information, visit www.avayanetwork.com, and click “Global Support Organization (GSO)”.

Chapter 4

CLI – Architecture, Access & Conventions

This chapter describes the P332G-ML CLI architecture and conventions, and provides instructions for accessing the P332G-ML for configuration purposes.

The configuration procedure involves establishing a Telnet session or a serial connection and then using the P330's internal CLI. The CLI is command-line driven and does not have any menus. To activate a configuration option, you must type the desired command at the prompt and press Enter. You can also configure your P332G-ML using the P330 Manager with its graphical user interface. For details, see the P330 Device Manager Appendix and the Avaya Multi-Service Network Manager P330 Device Manager User Guide on the Documentation and Utilities CD.

CLI Architecture

The P330 stack supports both Layer 2 switching and Layer 3 switching.
The P332G-ML CLI includes two CLI entities to support this functionality.

- The Switch CLI entity is used to manage Layer 2 switching of the entire stack. The Switch CLI entity is identical to the CLI of a P330 Layer 2 modules. CLI commands for managing Layer 2 switching are described in Chapter 6.
- The Router CLI entity is used to manage Layer 3 switching of a single module. The Router CLI entity exists in P330R and P332G-ML Layer 3 modules and supports different sets of commands depending on the device mode of the module.

Router mode commands are described in Chapter 8.

If the P332G-ML module is the Master of the stack, then the Switch CLI entity and the Router CLI entity co-exist on the same module.

To switch between the entities, use the **`session`** command. Refer to P330 Sessions.

Configuration of the **`password`** commands and **`community`** commands in one entity is automatically attributed to the other entity in the stack.

Initial access to the stack can be established via a serial connection or a Telnet connection to any one of the entities.

Establishing a Serial Connection

Perform the following steps to connect a terminal (physical or emulation) to the P330 Master Switch Console port for configuration of Stack or Router parameters:

1 Use the serial cable supplied to attach the RJ-45 console connector to the Console port of the P330 Master Switch. Connect the DB-9 connector to the serial (COM) port on your PC / terminal.
2 Ensure that the serial port settings on the terminal are 9600 baud, 8 bits, 1 stop bit and no parity.
3 When you see the "Welcome to P330" menu and are prompted for a Login Name, enter the default login. The default login is **`root`**.
4 When you are promoted for a password, enter the user level password **`root`**.
5 Now you can establish a connection to the Router or the Master switch (indicated when the SYS front panel LED is ON) using the Session commands (see P330 Sessions for details) and begin the configuration of Module, Stack or Router parameters.

Establishing a Telnet Connection

Perform the following steps to establish a Telnet connection to the P332G-ML for configuration of Stack or Router parameters. You can Telnet either the Stack Master IP address or directly to one of the Router IP address:

1 Connect your station to the network.
2 Verify that you can communicate with the P332G-ML using Ping to the IP of the P332G-ML. If there is no response using Ping, check the IP address and default gateway of both the P332G-ML and the station (see Assigning P330's IP Stack Address page 37 and Assigning P332G-ML Initial Parameters for Router Mode on Page 38).

Note: The P332G-ML default IP address is 149.49.35.**214** and the default subnet mask is 255.255.255.0.

3 From the Microsoft Windows® taskbar of your PC click **Start** and then **Run** (or from the DOS prompt of your PC), then start the Telnet session by typing:
`telnet` *`<P330_IP_address>`*
For example: **`telnet 149.49.35.214`**
4 If the IP Address in Telnet command is the IP address of the stack, then connection is established with the Switch CLI entity of the Master module. If you want to connect to the Router CLI entity, use the session command. If the IP address in the Telnet command is of the router, connection is established to the Router CLI entity in the router module.

5 When you are prompted for a Login Name, enter the default name **root**
6 When you are prompted for a password, enter the password **root** in lower case letters.
7 You can now configure the P330 stack and change its default IP address.

Command Line Prompt

Four factors affect the command line prompt:

- Host name of the CLI entity - the host name is used as the prefix of the command prompt (refer to hostname command on page 132).
- Module Number - counting from the bottom up used as part of the prefix. In this document the Module number in the prompt is generic and is represented by "N".
- Security level - used as the suffix of the prompt (Refer to Security Level on page 220.)
- Application context - used as body of the prompt, this part is not mandatory.

Example:

Host name of the router is City
Router is module number three
Application context is OSPF

The command line prompt looks as follows:

```
City-3(configure router:ospf)#
```

When you start the CLI, the initial prompt shows the number of the Master module in the P330 stack. For example, if the stack Master is Module 5, counting from the bottom up, then the prompt is:

```
P330-5>
```

In this document the Module number in the prompt is generic and is represented by "N".

If you wish to open a session with a P332G-ML routing module in the stack or reopen a session with the Master module, use the `session` command (see below).

The command prompt is *not* hierarchical in structure. If you wish to use several commands, each beginning with the same keyword, you must retype all parts of the command each time. For example, if after you want to set the system contact and the system name you must type both `set system contact` and `set system name`. However, you can use command abbreviations – see page 223.

P330 Sessions

You can use sessions to switch between P330 modules or to switch between Layer 2 and Layer 3 commands in the P332G-ML CLI.

To switch between P330 modules use the command:
`session [<mod_num>] <mode>`.

The <mod_num> is the number of the module in the stack, counting from the bottom up. The <mode> can be either **switch** or **router**. When Module Number is not specified, the command switches between the modes in the local module. Use **switch** mode to configure layer 2 commands. Use **router** mode to configure routing commands.

Examples:

To configure router parameters in the module that you are currently logged into, type the following command:

`session router`.

To configure the switch parameters, on module 6, type the command:
`session 6 switch`.

Note: When you use the `session` command the security level stays the same.

Security Levels

There are four security access levels – User, Privileged, Configure and Supervisor.

- The User level is a general access level used to show system parameter values.
- The Privileged level is used by site personnel to access stack configuration options.
- The Configure level is used by site personnel for Layer 3 configuration.
- The Supervisor level is used to define user names, passwords, and access levels of up to 10 local users.

A login name and password are always required to access the CLI and the commands. The login names and passwords, and security levels are established using the `username` command (see 116)

Switching between the entities, does not effect the security level since security levels are established specifically for each user. For example, if the operator with a privileged security level in the Switch entity switches to the Router entity the privileged security level is retained.

Entering the Supervisor Level

The Supervisor level is the level in which you first enter the CLI and establish user names for up to 10 local users. When you enter the Supervisor level, you are asked for a Login name. Type `root` as the Login name and the default password `root` (in lowercase letters):

```
Welcome to P330
Login: root
Password:****
Password accepted.
P330-N(super)#
```

Defining new users

Define new users and access levels using the `username` command in Supervisor Level. (see page 116).

Exiting the Supervisor Level

To exit the Supervisor level, type the command `exit`.

Entering the CLI

To enter the CLI, enter your username and password. Your access level is indicated in the prompt as follows:

The User level prompt is shown below:

```
P330-N>
```

The Privileged level prompt is shown below:

```
P330-N#
```

The Configure level prompt for Layer 3 configuration is shown below:

```
P330-N(configure)#
```

The Supervisor level prompt is shown below:

```
P330-N(super)#
```

Entering the Technician Level

This level can only be accessed from the Privileged and Supervisor levels and not from the User level.

This feature is not documented and is for use by Avaya Technical Support only.

Conventions Used

The following conventions are used in this chapter to convey instructions and information:

- Mandatory keywords are in boldface.
- Variables that you supply are in pointed brackets <>.
- Optional keywords are in square brackets [].
- Alternative but mandatory keywords are grouped in braces {} and separated by a vertical bar |.
- If you enter an alphanumeric string of two words or more, enclose the string in inverted commas.
- Information displayed on screen is displayed in `text` font.

Navigation, Cursor Movement and Shortcuts

The CLI contains a simple text editor with these functions:

Table 4.1 Navigation, Cursor Movement and Shortcuts

Keyboard	Functions
Backspace	Deletes the previous character
Up arrow / Down arrow	Scrolls back and forward through the command history buffer
Left arrow / Right arrow	Moves the cursor left or right
Tab	Completes the abbreviated command. Type the minimum number of characters unique to the command. An exception is the Reset System command which you must type in full.
Enter	Executes a single-line command
“ “	If you type a name with quotation marks, the marks are ignored.

Getting Help

On-line help may be obtained at any time by typing a question mark (**?**), or the word **`help`** on the command line or by pressing the F1 key. To obtain help for a specific command, type the command followed by a space and a question mark. Example: `Router>` **`show?`**

Command Syntax

Commands are not case-sensitive. That is, uppercase and lowercase characters may be interchanged freely.

Command Abbreviations

All commands and parameters in the CLI can be truncated to an abbreviation of any length, as long as the abbreviation is not ambiguous. For example, `version` can be abbreviated `ver`.

For ambiguous commands, type the beginning letters on the command line and then use the Tab key to toggle through all the possible commands beginning with these letters.

Universal Commands

Universal commands are commands that can be issued anywhere in the hierarchical tree.

Retstatus command

Use the `retstatus` command to show whether the last CLI command you performed was successful. It displays the return status of the previous command.

The syntax for this command is: **`retstatus`**

Tree command

The `tree` command displays the commands that are available at your current location in the CLI hierarchy.

The syntax for this command is: **`tree`**